UTILIZAÇÃO DA METODOLOGIA “RAMS” NA ANÁLISE DE BARREIRAS DE SEGURANÇA DE INSTALAÇÕES INDUSTRIAIS DE RISCO ELEVADO

José Augusto da Silva Sobral

Dissertação apresentada na Faculdade de Engenharia da Universidade do Porto
para obtenção do título de Doutor

Orientador: Prof. Doutor Luis António de Andrade Ferreira

PORTO
2010

“*Existe o risco que você não pode jamais correr, e existe o risco que você não pode deixar de correr*”

(Peter Drucker)

“*A parte que ignoramos é muito maior que tudo quanto sabemos*”

(Platão)

À minha esposa Ana Luisa e aos meus filhos David Alexandre e Ana Sofia, minhas grandes fontes de motivação.

RESUMO

Nas sociedades modernas é cada vez mais notória a necessidade de controlar ou gerir o risco. Esta preocupação encontra-se presente nas mais diversas actividades, abrangendo áreas desde as simples questões pessoais e quotidianas até às mais complexas e exigentes instalações industriais.

Em matéria de segurança podemos actuar no campo da prevenção ou no campo da protecção. No primeiro caso estamos a diminuir a probabilidade de ocorrência de um determinado acontecimento indesejável, enquanto no segundo os esforços vão no sentido de diminuir ou mitigar as consequências desse mesmo acontecimento. Na realidade, por muita prevenção que se possa fazer nunca se consegue evitar por completo a ocorrência de determinadas situações potencialmente perigosas. Desta forma, surge a necessidade de se instalarem barreiras de segurança para fazer face a esses acontecimentos.

Embora demonstrada e unanimemente aceite a importância dos equipamentos ou sistemas denominados barreiras de segurança, verifica-se no entanto uma quase inexistência de estudos ou análises quanto à sua fiabilidade, manutibilidade ou disponibilidade.

É neste sentido que se desenvolveu o presente trabalho, recorrendo aos conceitos e à filosofia da Metodologia RAMS (*Reliability, Availability, Maintainability and Safety*), tendo sido proposto efectuar uma nova abordagem que, embora fazendo uso de técnicas de análise já existentes, incorporasse também novas ferramentas. Desta forma, criou-se um modelo susceptível de ser adaptado a qualquer barreira de segurança, determinando a sua probabilidade de sucesso sempre que a mesma venha a ser solicitada.

Assim, foi criada e desenvolvida a Metodologia RODS (*Reliability Of Dormant Systems*), que permite uma análise da indisponibilidade de determinados items necessários na fase de arranque deste tipo de sistemas, obtendo-se como resultado o conhecimento do risco potencial para cada caso particular. Caberá depois aos técnicos ou responsáveis pela

gestão das instalações definir um critério para aceitação do risco e, no caso do mesmo não ser tolerável, criar os mecanismos que levem à sua redução.

Foi também demonstrada a metodologia proposta, tendo como alvo de aplicação uma barreira de segurança específica. Desta aplicação prática retirou-se importante informação qualitativa, assim como valores que permitem poder decidir de uma forma sustentada sobre potenciais acções no domínio da exploração e manutenção da barreira de segurança em causa.

Palavras-chave

Árvore de Falhas, Barreira de Segurança, Disponibilidade, *Dormant*, Fiabilidade, Manutibilidade, RAMS, Risco, Segurança

ABSTRACT

In our modern societies there's a necessity to control and manage risk. This concern is present in a huge diversity of activities, since our daily and personnel actions to complex and intricate industrial facilities.

In safety we can act in two fields, prevention and protection. The first is related to the attempt to decrease the probability of occurrence of an undesirable event while in the later the efforts are directed for trying to decrease or mitigate the consequences of such event. Reality shows that whatever the amount of prevention we cannot avoid at all the occurrence of situations considered potentially dangerous. So, it's then justified the installation of safety barriers just to face these events.

Although demonstrated and unanimous accepted the importance of these safety barriers, the truth shows few studies or analysis concerning its reliability, maintainability and availability.

The present work was developed in this scope, regarding all aspects and philosophy of RAMS Analysis (*Reliability, Availability, Maintainability and Safety*). The proposal was to create a new approach using well known techniques and incorporating new tools. So, it was built a model that could be used for any safety barrier, just to determine its success probability each time a demand occurs.

The RODS Methodology (*Reliability Of Dormant Systems*) was created and developed, allowing to know the unavailability of specific items that are necessary in the start-up phase of these kind of systems. The result of such methodology is the acquisition of the potential risk for each particular case. Then, industrial technicians and managers must define a risk acceptance criterion and, when not tolerable, create the mechanisms necessary to its reduction.

The RODS Methodology is demonstrated for a specific safety barrier. From this application some qualitative results came up as well as unavailability values allowing to

decide in a sustainable mode about possible actions in the operation and maintenance of a safety barrier.

Keywords

Availability, Dormant, Fault Trees, Maintainability, RAMS, Reliability, Risk, Safety, Safety Barriers

Dans les sociétés modernes il est de plus en plus évident qu'on besoin de contrôler ou de gérer les risques. Cette préoccupation est présente dans une variété d'activités couvrant des domaines de nôtre vie quotidienne à la plus complexe et éxigeant des installations industrielles.

Dans ce qui concerne à la sécurité il est possible d'agir dans la prévention ou dans le domaine de la protection. Dans le premier cas, nous réduisons la probabilité d'un événement indésirable particulier, tandis que le second testament efforts pour réduire ou atténuer les conséquences de cet événement. En fait, pour toute la prévention qu'il est possible faire on ne peut pas éviter totalement l'apparition de certaines situations potentiellement dangereuses. Ainsi naît le besoin d'installer barrières de sécurité pour faire face à ces événements.

Bien qu'il a été montré et acceptée à l'unanimité l'importance des équipements ou systèmes connus par barrières de sécurité, il n'y a pas beaucoup d'études ou des analyses quant à sa fiabilité, la maintenabilité et de disponibilité.

C'est ce sens que nous avons élaboré le présent ouvrage, en utilisant les concepts et la philosophie de la méthodologie RAMS (*Reliability*, *Availability*, *Maintainability and Safety*) a été proposé de procéder à une nouvelle approche qui, tout en utilisant des techniques déjà existantes, intègre également de nouveaux outils. Ainsi, il a été construit un modèle qui peut être adapté à n'importe quelle barrière de sécurité, déterminer ses chances de succès lorsque la même sera demandée.

Ainsi, a été créé et développé la méthodologie RODS (*Reliability Of Dormant Systems*), qui permet une analyse de l'indisponibilité de certains composants requis pour les start-ups de tels équipements, et ensuite l'obtention de la connaissance du risque potentiel dans chaque cas particulier. Il appartient ensuite à la gestion des locaux de définir un critère pour l'acceptation du risque et, s'il ne peut pas être toléré, de créer les mécanismes qui conduisent à sa réduction.

La méthodologie qui a été developpé au cours de ce travail a été appliquée dans le cas d’une barrière de sécurité. Cette application pratique permis d’obtenir de l'information qualitative importante, ainsi que des valeurs qui aident à décider sur une base soutenue sur les actions possibles dans le fonctionnement et le maintien de la barrière de sécurité concernés.

Mots Clé

Arbre de Fautes, Barrière de Sécurité, disponibilité, *dormant*, fiabilité, maintenabilité, RAMS, Risque, Sécurité

AGRADECIMENTOS

Os meus agradecimentos vão para todos que acreditaram em mim, e de uma forma ou de outra me ajudaram a completar esta etapa da minha vida.

- Em primeiro lugar gostava de agradecer ao Prof. Doutor Luis Andrade Ferreira, pela sua orientação. As suas opiniões pertinentes, conhecimento e experiência permitiram a realização do presente trabalho. Ao longo dos últimos anos tive o privilégio de com ele poder partilhar a realização de vários trabalhos académicos e participar em conferências nacionais e internacionais. O meu sincero e eterno agradecimento.

- Gostava também de agradecer aos meus colegas do Departamento de Engenharia Mecânica do ISEL (Instituto Superior de Engenharia de Lisboa), e em especial aos colegas da Secção de Engenharia Industrial e Manutenção, pelo incentivo e coragem que me deram ao longo deste trabalho.

- Aos meus amigos Luis Saleiro e João Ruivo, pelo estímulo e amizade demonstrada desde sempre.

- O meu agradecimento às Bombas Grundfos Portugal, nomeadamente ao seu administrador Doutor José Costa e ao Eng. Paulo Conceição por me facultarem alguns elementos referentes aos equipamentos estudados.

- O meu agradecimento à *Relex Software Corporation*®, e em especial a Horst Kuntscher (Alemanha), Cindy Lutz e Jake Moody (Estados Unidos da América) pela cedência do programa informático utilizado na aplicação prática da presente dissertação, e sem o qual não teria sido possível alcançar os resultados apresentados.

- Finalmente, mas não menos importante, à minha esposa Ana Luisa e aos meus filhos David Alexandre e Ana Sofia, que ao longo dos últimos anos me perguntavam porque estava sempre a trabalhar no computador. Agora já lhes posso dizer que em grande parte "*foi por isto!*"

ÍNDICE

LISTA DE SÍMBOLOS

Símbolo	Descrição
$R(t)$	Função fiabilidade
$F(t)$	Função probabilidade acumulada de falha
$M(t)$	Função manutibilidade
$A(t)$	Função disponibilidade
$\lambda(t)$	Função de risco ou função taxa de avarias
t	Variável tempo
$f(t)$	Função densidade de probabilidade de falha
$\Delta(t)$	Duração da missão
ρ	Coeficiente de correlação
k	Parâmetro de forma da distribuição Gama
$\Gamma(k)$	Função Gama
e^{μ}	Parâmetro de escala da distribuição Gama
γ	Parâmetro de posição ou vida inicial da distribuição de Weibull
β	Parâmetro de forma da distribuição de Weibull
η	Parâmetro de escala ou vida característica da distribuição de Weibull
μ	Média / Taxa de reparação
σ	Desvio padrão
z	Variável padronizada da distribuição Normal para $\mu=0$ e $\sigma=1$
$\mu`$	Média da distribuição Lognormal
$\sigma`$	Desvio padrão da distribuição Lognormal
n	Número de ensaios na distribuição Binomial
r	Número de insucessos na distribuição Binomial
p	Probabilidade de insucesso na distribuição Binomial
q	Probabilidade de sucesso na distribuição Binomial
$N_f(t)$	Número médio de avarias
N_0	Dimensão inicial da amostra
H_0	Hipótese nula do Teste de Laplace
H_1	Hipótese alternativa do Teste de Laplace
α	Nível de significância (Teste de Laplace) / Factor de adormecimento
$g(t)$	Função densidade de probabilidade de reposição em serviço
ε	Parâmetro de forma da função densidade de probabilidade de reposição

$Q(t)$	Indisponibilidade
τ	Intervalo de tempo entre inspecções, testes ou ensaios
τ_R	Tempo médio de reparação
λ_{DU}	Taxa de avarias para avarias perigosas não detectadas
λ_{DD}	Taxa de avarias para avarias perigosas detectadas
λ_{2v}	Taxa de avarias do componente 2 em vazio
λ_{2c}	Taxa de avarias do componente 2 em carga
λ_{DCa}	Taxa de avarias do detector-comutador na actuação
λ_{DCd}	Taxa de avarias do detector-comutador quando em detecção
ϕ	Taxa de solicitação do processo ou intensidade do acontecimento acidental

LISTA DE ACRÓNIMOS

- A -

AFNOR	Association Française de Normalisation
AGAN	As Good As New
ALARP	As Low As Reasonably Practicable
ALT	Accelerated Life Test
AMSAA	Army Material Systems Analysis Activity
ARAMIS	Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive
ASEP	Accident Sequence Evaluation Program

- B -

BBN	Bayesian Belief Network
BDD	Binary Decision Diagram
BN	Bayesian Network

- C –

CBFTA	Condition-Based Fault Tree Analysis
CCF	Common Cause Failures
CEA	Comité Européen des Assurances
Cepreven	Centro Nacional de Prevención de Daños y Pérdidas
CREAM	Cognitive Reliability and Error Analysis
CSP	Cold Spare

- D -

DFT	Dynamic Fault Tree
DFTA	Dynamic Fault Tree Analysis

- E -

EEI	Edison Electrical Institute
EN	European Norm
EPDM	Ethylene Propylene Diene Monomer (M-class)
ESD	Emergency Shutdown Systems
ET	Estatística de Teste
ETA	Event Tree Analysis

- F -

FDEP	Functional Dependency
FDT	Fractional Dead Time
FM	Factory Mutual
FMEA	Failure Modes and Effect Analysis
FPSF	Failure Probability-Safety Factor
FT	Fault Tree
FTA	Fault Tree Analysis
FTS	Fault Tolerant System

- G -

GA	Genetic Algorithms
GAMAB	Globalment Au Moins Aussi Bon
GTC	Gestão Técnica Centralizada

- H -

HALT	High Accelerated Life Test
HAZID	Hazard Identification
HAZOP	Hazard and Operability
HEART	Human Error Assessment and Reduction Technique
HPP	Homogeneous Poisson Process
HRA	Human Reliability Analysis
HSP	Hot Spare

- I -

IEC	International Electrotechnical Comittee
ISO	International Organization for Standardization

- J –

- K -

KTT	Kinetic Tree Theory

- L -

LC	Confidence Level
LOPA	Layer Of Protection Analysis

- M -

MC	Markov Chain
MCS	Minimal Cut Set
MDT	Mean Down-Time
MEM	Minimum Endogenous Mortality
MICSUP	Minimal Cut Set Upwards
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MLE	Maximum Likelihood Estimator
MOCUS	Method of Obtaining Cut Sets
MPS	Minimal Path Set
MPPS	Maintenance Personnel Performance Simulation
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTFF	Mean Time To First Failure
MTTR	Mean Time To Repair
MUT	Mean Up-Time

- N -

NFPA	National Fire Protection Association

NHPP	Non Homogeneous Poisson Process
NP EN	Norma Portuguesa European Norm
NS	Norsok Standard
NSWC	Naval Surface Warfare Center

- O -

OREDA	Offshore Reliability Data
OT	Ordem de Trabalho

- P -

P&I	Piping and Instrumentation Diagram
PAND	Priority AND
PFOD	Probability of Failure On Demand
PHA	Preliminary Hazard Analysis
PN	Petri Nets (Redes de Petri)
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment

- Q -

QRA	Quantitative Risk Assessment
QRS	Quadro Repetidor de Sinais

- R -

RAC	Rome Air Development Center
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAMS+C	Reliability, Availability, Maintainability, Safety and Costs
RBD	Reliability Block Diagram
RCA	Root Cause Analysis
RIA	Rede de Incêndios Armada
ROCOF	Rate of Ocurrence of Failures
RODS	Reliability Of Dormant Systems

RRR Rapid Risk Ranking

- S -

SADI Sistema Automático de Detecção de Incêndios

SEQ Sequential Enforcing

SFF Safe Failure Function

SFL Sequential Failure Logic

SIL Safety Integrity Level

SIS Safety Instrumented System

- T -

TESEO Technique for Empirical Simulation of Errors in Operations

THERP Technique for Human Error Rate Prediction

TTF Time To Failure

TTR Time To Repair

- U -

UL Underwriters Laboratories

- V -

VP Valor de Prova

- W -

WSP Warm Spare

- X –

- Y –

- Z -

ZBDD Zero-Supressed Binary Decision Diagrams

LISTA DE FIGURAS

LISTA DE TABELAS

CAPÍTULO I

INTRODUÇÃO

1.1 – Enquadramento

Desde o início da história que a Humanidade tem sempre tentado prever o futuro com base em determinadas observações. Alguns dos métodos usados passavam por observar o voo das aves, o movimento das folhas das árvores ou a cor do céu, tentando daí inferir ou prognosticar acontecimentos futuros.

Hoje em dia, a Engenharia já não necessita de tais métodos nem de bolas de cristal para prever o "futuro" dos seus bens. Através da análise de dados de vida reais, ensaios laboratoriais ou técnicas de simulação, os profissionais de fiabilidade conseguem determinar a probabilidade de componentes, unidades, sistemas e equipamentos poderem realizar as suas funções durante determinadas missões, e sob condições específicas, sem que ocorram avarias nos mesmos.

Um bom diagnóstico, estimativa ou previsão de avarias pode levar à tomada das melhores decisões no âmbito da gestão dos bens, tendo significativo impacto ao nível da segurança, dos custos e, por vezes, até no ambiente.

Em instalações industriais de risco elevado, a gestão destes bens e o conhecimento do risco subjacente em cada situação particular, tem vindo a ocupar lugar de destaque nas preocupações dos responsáveis pelas instalações. Trata-se de um assunto de primeira ordem sempre que estejam em causa vidas humanas ou perdas económicas significativas.

1.2 – Motivação e Objectivos

A motivação para a realização do presente trabalho resulta da relação desenvolvida ao longo de quase duas décadas com uma actividade profissional na área da segurança contra incêndios, e da actividade de docência no ensino superior na área da Manutenção e Fiabilidade de componentes e sistemas.

Esta conjunção de experiências, por um lado de ordem prática, na tentativa de perceber o porquê da avaria dos equipamentos e interpretação das suas consequências, e por outro lado com a aquisição de conhecimento teórico sobre modelos e metodologias de análise existentes, levou a que se tentasse efectuar uma ponte entre estas duas vertentes, no sentido de estabelecer uma abordagem ou metodologia que fosse suficientemente prática e ao mesmo tempo cientificamente sólida para o tratamento e análise de equipamentos reais, designados por barreiras de segurança.

Assim, o objectivo principal deste trabalho é apresentar uma metodologia de análise para os bens denominados barreiras de segurança, descrevendo um método de cálculo que permita determinar a disponibilidade deste tipo de sistemas, tendo em conta as suas especificidades.

1.3 – Contribuições da Tese

Relativamente ao tema são apresentadas algumas abordagens existentes, descrito o estado da arte em diversas matérias, proposta uma metodologia de análise e efectuada uma aplicação prática dessa metodologia, especificamente destinada a barreiras de segurança normalmente presentes na maioria das instalações industriais de risco elevado.

Pretende-se acima de tudo desenvolver algo que ultrapasse o conceito meramente teórico e matemático, apresentando um modelo com aplicabilidade, potenciando alguma inovação e a passagem de novas abordagens científicas para a prática do campo industrial.

Com este trabalho pretendeu-se também colmatar alguma lacuna existente a nível da investigação e desenvolvimento, nomeadamente sobre determinados equipamentos, que

pela sua condição e características funcionais não têm sido alvo de muitas análises no campo da fiabilidade, manutibilidade e disponibilidade.

Em termos científicos foram introduzidos conceitos relativamente recentes, como as portas lógicas dinâmicas, portas essas que se encontram inseridas na Análise de Árvore de Falhas Dinâmica (DFTA), sendo utilizadas para mostrar algumas dependências e sequências funcionais de componentes instalados num determinado sistema.

A grande contribuição do presente trabalho refere-se à apresentação de uma metodologia para análise de barreiras de segurança, não existente na bibliografia consultada, resultando numa nova abordagem ao problema. Este contributo revela-se de extrema importância, uma vez que proporciona um melhor conhecimento do comportamento deste tipo de bens, ajudando os responsáveis pela sua manutenção e exploração na tomada de decisões.

Nesta metodologia faz-se a distinção entre duas fases particulares de actuação destes equipamentos, nomeadamente uma primeira relacionada com a disponibilidade dos componentes de suporte (ou arranque) e uma segunda fase relativa à fiabilidade dos componentes activos durante um determinado período de tempo ou missão. Neste trabalho em particular dá-se ênfase à primeira fase, considerada fundamental no funcionamento de qualquer barreira de segurança.

Com o trabalho desenvolvido espera-se ter clarificado alguns assuntos, cujo conteúdo faz parte de algumas das unidades curriculares ministradas no ensino superior universitário e politécnico nas áreas da Engenharia Mecânica, ter construído uma ferramenta de suporte aos técnicos da indústria preocupados com a segurança e disponibilidade dos seus bens e dado um pequeno contributo para a comunidade científica que se interessa por áreas tão aliciantes como a Manutenção e a Fiabilidade, onde o desenvolvimento de metodologias pode propiciar novos campos de estudo científico.

1.4 – Estrutura da Tese

A tese encontra-se estruturada em sete capítulos, existindo uma interligação entre os mesmos através de uma lógica de sustentabilidade teórica dos conceitos. Houve também a necessidade de apresentar alguns anexos que complementam o corpo do documento.

No presente capítulo fez-se um enquadramento do tema, apresentou-se uma panorâmica sobre o assunto tratado, a motivação para a realização do trabalho e os objectivos propostos para o mesmo. Também se apontam alguns contributos que se espera terem sido introduzidos na área da fiabilidade, manutenção e segurança com a elaboração do presente estudo.

O **Capítulo II** serve para descrever o conceito RAMS (*Reliability*, *Availability*, *Maintainability and Safety*), a sua importância ao longo de todo o ciclo de vida de sistemas ou equipamentos e as suas implicações no risco. Relativamente a este conceito, são apresentadas as características principais sobre cada um dos elementos que o constituem, nomeadamente a Fiabilidade, Manutibilidade, Disponibilidade e Segurança. Na descrição das metodologias existentes para análise da fiabilidade de sistemas dá-se particular atenção à Análise de Árvore de Falhas e à necessidade de evolução das Árvores de Falhas estáticas para as Árvores de Falhas dinâmicas. A focalização nesta técnica justifica-se, uma vez que a mesma faz parte da metodologia proposta em capítulos subsequentes.

O **Capítulo III** tem a ver especificamente com o risco. Define-se o risco e metodologias de avaliação do mesmo, comparando o risco potencial com o considerado risco aceitável. Faz-se referência a critérios de aceitação como o ALARP, GAMAB ou MEM, apresentando-se a denominada "matriz de risco". É introduzida a noção de barreira de segurança, sua classificação e avaliação. Referem-se conceitos como o Nível de Integridade de Segurança (SIL = *Safety Integrity Level*), Sistemas Instrumentados de Segurança (SIS = *Safety Instrumented Systems*), Probabilidade de Falha quando Solicitado (PFOD = *Probability of Failure On Demand*) ou Análise de Camadas de Protecção (LOPA = *Layer Of Protection Analysis*). Neste capítulo é ainda abordado um tipo particular de risco, nomeadamente o risco de incêndio. Mostra-se a importância da temática da segurança contra incêndios, que tem vindo ao longo dos anos a suscitar um interesse crescente, no sentido de se encontrarem formas para controlar ou mitigar este tipo de acontecimento. Faz-se a diferenciação entre prevenção e protecção, enunciando os factores que contribuem para a existência de risco de incêndio, apontando as medidas de protecção como forma de minimizar a gravidade das suas consequências, onde as barreiras de segurança assumem papel fundamental. Apresentam-se algumas metodologias ou abordagens sobre o assunto, quer quanto à probabilidade de ocorrência, quer quanto às suas eventuais consequências.

No **Capítulo IV**, descrevem-se as particularidades inerentes aos bens que se encontram no estado "*dormant*", como é o caso das barreiras de segurança. Clarificam-se as diferenças entre o que se entende por um bem em armazém ("*storage*"), um bem em "*standby*" e um bem no estado "*dormant*". Analisam-se as designadas "falhas ocultas", normalmente presentes nas barreiras de segurança, e mostra-se como é importante a disponibilidade deste tipo de sistemas sempre que são solicitados, assim como a sua fiabilidade durante a restante missão. É dada especial atenção à fase de arranque das barreiras de segurança que se encontram no estado "*dormant*", e à importância da periodicidade das inspecções, testes ou ensaios, tendo este último aspecto um impacto significativo na probabilidade de falha do sistema quando solicitado (PFOD).

O **Capítulo V** serve para apresentar uma metodologia para análise de barreiras de segurança no estado "*dormant*", designada Metodologia RODS (*Reliability Of Dormant Systems*). Esta metodologia permite determinar a fiabilidade deste tipo de bens, com especial realce na fase de arranque, obtendo-se assim um indicador do maior ou menor sucesso desses sistemas quando são necessários. Através da construção de uma Árvore de Falhas e identificação dos acontecimentos básicos relativos aos componentes de suporte e suas interligações funcionais, é possível efectuar inicialmente uma análise qualitativa, sendo posteriormente realizada uma análise quantitativa e uma análise de sensibilidade.

No **Capítulo VI** demonstra-se a metodologia proposta no capítulo anterior, através de um exemplo prático. É descrito o sistema em estudo e realizada uma Análise de Árvore de Falhas (FTA), verificando a exequibilidade da primeira fase da metodologia RODS para este caso específico. É efectuada uma análise qualitativa, com a respectiva determinação dos conjuntos de corte mínimos, seguida de uma análise quantitativa, onde se determinam os valores de indisponibilidade para os acontecimentos básicos, acontecimentos intermédios e principalmente para o acontecimento de topo. Também se reveste de carácter de grande importância a análise de sensibilidade realizada, uma vez que permite detectar o contributo de cada situação para a ocorrência do acontecimento de topo. Neste capítulo também são simulados vários cenários, permitindo aos responsáveis pela gestão do risco tomar as melhores decisões, tendo em conta o critério de aceitação estipulado.

Finalmente, no **Capítulo VII**, são apresentadas conclusões e apontadas algumas perspectivas de trabalhos futuros, com base no trabalho desenvolvido.

CAPÍTULO II

CONCEITO “*RAMS*”

2.1 – Introdução

O mundo está a passar por mudanças de tecnologia cada vez mais rápidas. Este rápido desenvolvimento, aliado ao crescente aumento da produção e globalização dos mercados, tem como consequência o aumento da competitividade à escala mundial, acarretando também um aumento dos padrões de consumo e segurança.

O referido aumento da concorrência empresarial e a globalização da economia fazem com que as empresas tenham passado a integrar outros objectivos além dos meramente económicos, visando a maximização do lucro. Estes passam por objectivos de natureza mais estratégica e vitais para a sua sobrevivência, como necessidades sociais, aspectos de segurança e de conforto dos colaboradores, ter mais preocupação com as questões ambientais, aumentar a qualidade dos produtos, construir relações mais fortes com os fornecedores e distribuidores, cuidar da imagem e prestigio da organização, cumprir a legislação, dar uma resposta rápida às necessidades do mercado, etc...

Assim, as empresas terão que encontrar meios para produzir ao custo mais económico, o que na maior parte das vezes passa por uma gestão eficaz dos seus activos, evitando as suas falhas ou resolvendo-as o mais rápido possível. Para que este objectivo seja alcançado são realizados novos estudos ou utilizadas metodologias de análise já testadas e comprovadas. Nesta vertente, quer nos estejamos a referir a simples componentes ou a sistemas complexos, quer sejam bens reparáveis ou bens descartáveis, ou independentemente da fase do seu ciclo de vida sobre a qual incidem, os estudos referentes à **Fiabilidade**, **Disponibilidade** e **Manutibilidade** dos bens transmitem a

preocupação por parte da engenharia em optimizar determinados processos e estabelecer novas abordagens. Desta forma, muitas metodologias e ferramentas têm surgido e obtido êxito ao longo dos últimos anos, ajudando quem se interessa por estas áreas na tomada de decisões.

Desde então, e devido à afinidade entre as três áreas citadas, têm sido realizados nas últimas décadas diversos estudos e simpósios internacionais sobre a temática RAM (*Reliability*, *Availability and Maintainability*).

Mais recentemente, com a introdução de um quarto conceito, designado por **Segurança** operacional ou de funcionamento, estes temas foram de certa forma agrupados num acrónimo denominado **RAMS** (*Reliability*, *Availability*, *Maintainability and Safety*). O RAMS é uma característica de exploração de um sistema e é alcançado através da aplicação de conceitos de engenharia, métodos, ferramentas e técnicas estabelecidas ao longo de todo o ciclo de vida do sistema ou equipamento, implicando consequências sobre o risco. O acrónimo RAMS é uma combinação de fiabilidade, disponibilidade, manutibilidade e segurança de funcionamento de um sistema, e das suas interacções. Pode ser assim caracterizado como sendo um indicador qualitativo e quantitativo do grau de fiabilidade em que o sistema, ou os subsistemas e componentes que integram o sistema, possam funcionar como requerido, estando ao mesmo tempo disponível e sendo seguro (NP EN 50126, 2000) (Sobral, 2003).

Desta forma, as actividades de Manutenção tornaram-se uma área vital no alcançar de muitos dos objectivos enunciados, assistindo-se cada vez mais à preocupação das empresas em integrar no processo de aquisição de um dado equipamento, logo na fase de elaboração do seu Caderno de Encargos, um conjunto de especificações para além das meramente técnicas, estabelecendo limites (mínimos) considerados aceitáveis para a Fiabilidade, Disponibilidade, Manutibilidade e Segurança.

De acordo com a NP EN 50126 (2000), "*Os objectivos de segurança e de disponibilidade de um sistema em funcionamento só podem ser alcançados se estiverem satisfeitos todos os requisitos de fiabilidade e de manutibilidade e se as actividades de manutenção e de exploração forem controladas ao longo do ciclo de vida do sistema, assim como o meio ambiente em que se insere*". Assim, o RAMS é um método ou abordagem que integra as características de fiabilidade, manutibilidade, disponibilidade e segurança de um bem, ou seja, é uma metodologia que visa a redução dos custos e ao mesmo tempo a diminuição dos riscos.

O ciclo de vida dos sistemas, com as suas fases individuais e as suas interligações, pode ser representado em forma de esquema. A Figura 2.1 é uma das várias representações do ciclo de vida (NP EN 50126, 2000).

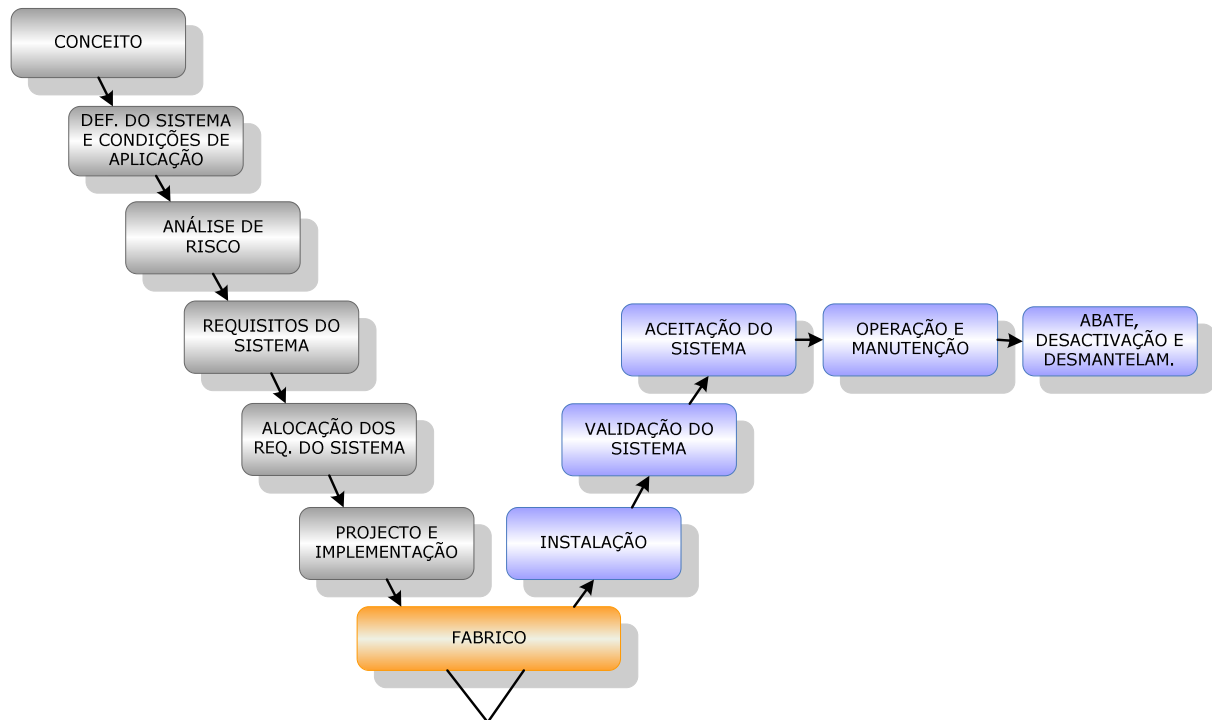



Figura 2.1 – Representação em "V" do ciclo de vida dos sistemas
[Fonte: NP EN 50126 (2000)]

A ramificação do topo para a base (no lado esquerdo) designa-se por desenvolvimento, finalizando com o fabrico dos componentes do sistema. A ramificação da base para o topo (no lado direito) refere-se à montagem, instalação, recepção e exploração de todo o sistema. A representação em "V" pressupõe que as actividades de aceitação estão intrinsecamente ligadas às actividades de desenvolvimento, pois tudo que foi projectado deve ser verificado face aos requisitos iniciais.

Mais recentemente, as análises RAMS têm sido aplicadas em diversos campos, como no desenvolvimento, teste e avaliação operacionais de sistemas de defesa militar (Jackson *et al*, 2005), na integração com análises de risco nos processos de manutenção, com vista à diminuição da frequência de avarias, das suas consequências e custos de manutenção (Eti *et al*, 2007), utilizando igualmente ferramentas relativamente recentes para a sua própria modelação, como é o exemplo de redes neuronais artificiais (Rajpal *et*

al, 2006) e algoritmos genéticos (Martorell *et al*, 2007) (Marseguerra *et al*, 2006) (Martorell *et al*, 2005), ou inclusivamente usando as análises RAMS para modelar o desempenho de sistemas considerados críticos (Sharma & Kumar, 2008), ou sistemas tolerantes à falha (Wang *et al*, 2007). Coulibaly et al (2008) descrevem uma metodologia para determinar os indicadores RAMS numa fase inicial de projecto de produtos mecânicos, servindo-se deles para tirar vantagens competitivas. Outro estudo (Torres-Echeverría *et al*, 2009) mostra como também nesta fase do ciclo de vida se pode optimizar um sistema instrumentado de segurança (SIS=*Safety Instrumented System*), baseado numa análise RAMS+C (C=*Costs*), nomeadamente para cumprir determinados requisitos normativos.

Alguns dos estudos dirigem-se fundamentalmente à área da manutenção, com o objectivo de redução de custos e/ou riscos (Baptista & Dias, 2007). Algumas variantes ao RAMS foram desenvolvidas, como por exemplo num estudo onde o significado do acrónimo RAM foi modificado, correspondendo a "*Reliability*, *Availability* and *Maintenance*" (Herder *et al*, 2008).

2.2 – Importância da Fiabilidade e Manutibilidade na Disponibilidade e Segurança operacional

Tendo em conta todo o ciclo de vida de um bem, e tendo como objectivo a tomada das melhores decisões em qualquer uma das suas fases, recorre-se a diversos processos, quer na fase de selecção desse bem, através da análise da rentabilidade do investimento, quer na fase de exploração, seleccionando as melhores políticas de manutenção e introdução de melhorias, ou até mesmo na fase de desactivação, através da análise do melhor momento para se proceder à substituição ou abate do equipamento.

Estas decisões fundamentam-se em conceitos básicos de fiabilidade e manutibilidade, assentando na maioria dos casos em princípios de racionalidade económica. No que respeita à fiabilidade, analisa-se e estima-se a frequência com que o bem irá avariar, resultado de algumas características intrínsecas (projecto e fabrico) e de algumas características extrínsecas (condições de carga, condições ambientais), enquanto no campo da manutibilidade se pondera a aptidão do bem para ser sujeito a manutenção, como por exemplo a facilidade de acesso, a ergonomia ou a segurança.

Todas as características anteriormente enunciadas vão, de uma forma ou outra, influenciar a percentagem de tempo em que o bem se encontra efectivamente em condições para cumprir a sua função ou a probabilidade do mesmo se encontrar em condições operacionais num momento futuro, ou seja, a sua disponibilidade operacional.

Desta forma, ter-se-á em conta o tempo médio de bom funcionamento entre intervenções de manutenção (MUT = *Mean Up-Time*) e o tempo médio de intervenção para restabelecer as condições de bom funcionamento (MDT = *Mean Down-Time*), incluindo os tempos relativos a procedimentos administrativos e logísticos. Caso não se considerem estes últimos, a característica analisada designar-se-á por disponibilidade intrínseca. Em qualquer dos casos, a combinação de níveis elevados de fiabilidade e de manutibilidade tem como resultado altos índices de disponibilidade do bem.

Por outro lado, quando os modos de falha presentes num determinado bem podem conduzir à ocorrência de potenciais acidentes, pondo em causa a integridade física de quem se encontre na sua próximidade, ou eventualmente causando danos graves no ambiente (perda de fluído ou emissão de gases), também a fiabilidade e a manutibilidade serão aspectos fundamentais a ter em conta, estimando-se a probabilidade de falha do bem e a facilidade e consequente rapidez com que se essa falha é anulada, relacionando-se desta forma estes dois factores também com o conceito de segurança.

Para compreender com mais profundidade cada um dos temas inerentes ao conceito RAMS, os próximos parágrafos visam detalhar cada um dos elementos que o constituem, servindo também como base teórica para o trabalho realizado no presente documento.

2.3 – Conceito de Fiabilidade

Prever o futuro sempre foi uma das tentativas do homem, a maior parte das vezes fazendo-o através da observação de determinados acontecimentos e comportamentos e daí tentando adivinhar o que poderia acontecer. Naturalmente estas tentativas de previsão apresentam hoje uma incerteza muito menor da que se verificava no passado, graças à evolução dos métodos e ferramentas actuais ao dispor dos técnicos para tratar a informação referente aos dados recolhidos.

Os métodos de análise de fiabilidade (e risco) desenvolveram-se fortemente ao longo dos últimos anos, tendo-se começado a efectuar este tipo de estudos durante a Segunda

Guerra Mundial, abordando questões relacionadas com o desempenho de componentes e sistemas durante as missões aéreas (Estados Unidos) ou com a probabilidade de falha do sistema de mísseis (Alemanha), passando posteriormente por outras áreas como a espacial ou as instalações nucleares e generalizando-se, por fim, a outros tipos de indústria. Uma descrição completa da história, desenvolvimento e objectivos da engenharia da fiabilidade (desde 1941 até 1986) pode ser analisada na obra publicada por Kececioglu (2002).

Questões como: "***Durante quanto tempo o equipamento é capaz de funcionar sem falhar?***" ou "***Qual é o momento adequado para fazer a substituição de determinado componente, antes que o mesmo falhe?***" são perguntas que o estudo da fiabilidade tenta responder, utilizando para isso ferramentas matemáticas, designadas por modelos estatísticos.

A informação referente à vida de componentes, órgãos, subsistemas ou sistemas tem a ver com a duração ou período de tempo de operação bem sucedida, ou o tempo decorrido até se verificar determinada avaria.

Neste momento interessa desde já ressalvar dois aspectos importantes que podem ajudar na clarificação de alguns conceitos que são descritos ao longo do texto do presente trabalho, nomeadamente:

- A noção de "tempo", que pode ter várias interpretações e vários tipos de unidades de medida, podendo ser expresso em horas, ciclos, quilómetros, número de actuações, etc., havendo a necessidade de definir e clarificar bem estas unidades de medida em qualquer estudo que se efectue. Qualquer informação desta natureza poderá ser tratada em termos de análise e previsão de comportamento como uma análise de dados de vida de um determinado bem;
- A diferença entre "falha" e "avaria", que muitas vezes é referida indistintamente, mas que, de acordo com a NP EN 13306 (2007), deverá ser utilizada de forma adequada. Deste modo, ao longo do trabalho os dois termos serão usados tendo em consideração as suas definições, nomeadamente:

  "*Avaria – Cessação da aptidão de um bem para cumprir uma função requerida. Depois da avaria o bem poderá estar em falha, total ou parcial. "Avaria" é um acontecimento. "Em falha" ou "avariado" é um estado.*"

> *"Em falha – Estado de um bem inapto para cumprir uma função requerida, excluindo a inaptidão devida à manutenção preventiva ou outras acções programadas, ou devida à falta de recursos externos."*

Assim, ao longo do texto quando se estiver a referir a inaptidão de um bem para o cumprimento de uma dada função, será utilizado o termo "avaria" ou os termos "em falha" ou "avariado", conforme a referência corresponda a um acontecimento ou um estado, respectivamente.

Nem todas as análises aos dados de vida são de idêntico grau de dificuldade. Repare-se, por exemplo, a difícil tarefa de prever para um determinado indivíduo quando ocorrerá a sua morte ou o surgimento de uma doença grave, apesar de estatisticamente poder haver análises que apontam idades médias de vida ou probabilidades de ocorrência de determinada doença consoante a idade desse mesmo indivíduo.

A par da necessidade de clarificação das unidades de medida de vida também é necessário definir o que constitui uma avaria para estas unidades. O que pode à primeira vista ser uma constatação óbvia, quando não tratada de forma rigorosa poderá invalidar os resultados de análises e testes, muitas vezes traduzidos por custos elevados.

De uma forma geral, a fiabilidade pode ser definida como uma ciência que fornece as ferramentas teórico-práticas, onde a probabilidade e capacidade de componentes, sistemas ou equipamentos para satisfazer as funções requeridas durante determinados períodos de tempo sem avaria, em ambientes específicos, e dentro de certos intervalos de confiança, podem ser especificadas, projectadas, previstas, testadas e demonstradas.

Pode-se complementar a definição de fiabilidade com recurso à vasta literatura existente. De acordo com a recente norma portuguesa sobre terminologia da manutenção, a NP EN 13306 (2007), fiabilidade é a "***Aptidão de um bem para cumprir uma função requerida sob determinadas condições, durante um dado intervalo de tempo***", onde "***O termo fiabilidade também é utilizado como uma medida de desempenho da fiabilidade e poderá também ser definido como uma probabilidade***".

De acordo com outras fontes, a fiabilidade também é referida como uma "***medida da probabilidade de sucesso no desempenho de um sistema durante um período de tempo***" (Andrews & Moss, 2002) ou a "***capacidade de um item realizar uma função***

requerida, sob determinadas condições ambientais e operacionais durante um dado período de tempo" (Rausand & Hoyland, 2004).

Na norma francesa AFNOR X 06-501, citada por Monchy (1996), a definição de fiabilidade é dada como "***A característica de um dispositivo expressa pela probabilidade que esse dispositivo cumpra uma função requerida nas condições de utilização e por um período de tempo determinado***".

Em todas estas definições sobressaem alguns elementos (ou palavras-chave) significativos, e que são comuns em praticamente toda a bibliografia consultada, nomeadamente:

- Probabilidade;
- Função;
- Condições;
- Tempo.

Estes elementos são de grande importância para os estudos de fiabilidade, daí se dispensar nas próximas linhas alguma atenção aos mesmos de forma isolada.

Probabilidade – A fiabilidade é uma probabilidade. É essa probabilidade que caracteriza a diferença entre equipamentos da mesma natureza. A probabilidade permite-nos saber o quanto é a aptidão de um bem para funcionar sem falha durante um certo tempo, indicando também a existência de um grau de incerteza associado a esse cálculo, que é devido em grande parte à variabilidade existente em qualquer ramo da Engenharia. A probabilidade é uma quantificação subjectiva da incerteza para suportar uma decisão.

Função – Antes do início de qualquer estudo de fiabilidade deve-se definir bem aquilo que se chama "*desempenhar uma função*" e indicar de que função se trata. O nível em que essa função é desempenhada pode ser definido pelo tipo de acontecimento ou estado. Podem-se distinguir os seguintes tipos de avaria:

- De acordo com o grau de influência na capacidade de trabalho (em falha total ou parcial);
- Através do carácter físico de aparecimento da avaria (catastrófica = avaria repentina e completa ou paramétrica = gradual);
- Se é independente (primária) ou dependente (secundária) de outras avarias;
- Quanto ao tempo de existência em falha (estável, temporária ou intermitente).

Condições – É outro aspecto que também deve ser cuidadosamente definido. O tipo de aplicação, condições ambientais e outros factores diferenciadores em que o equipamento vai operar podem ter um impacto nos valores de fiabilidade a determinar. Neste contexto importa especificar bem qual o tipo de fiabilidade que está a ser avaliado; se é a fiabilidade intrínseca (em bancos de teste, com condições bem controladas) ou se é a fiabilidade operacional (nas condições reais de uso).

Tempo – Há que distinguir se estamos a falar de bens que devem funcionar um certo tempo, de bens que funcionam intermitentemente ou uma única vez (duração de uma missão, número de ciclos, quilometragem, etc.) ou se são bens em cuja utilização não se observa a intervenção do tempo (explosivos).

A fiabilidade, à semelhança da manutibilidade (em bens reparáveis), cobre todos as fases da vida de um produto, desde a sua concepção, projecto e produção, assim como durante o tempo de vida em que é explorado e mantido. O conceito de manutibilidade, ligado à maior ou menor facilidade com que as acções de manutenção sobre os bens são realizadas, será melhor definido num próximo parágrafo (ver 2.4).

Mas como se pode inserir a fiabilidade na política de uma empresa?

Normalmente a fiabilidade baseia-se nos resultados de ensaios em fábrica ou no desempenho em campo, servindo estas fontes para medir e melhorar de forma apurada a fiabilidade dos bens.

No entanto, a concorrência e a evolução do mercado conduzem a uma constante redução de custos, o que poderá afectar a realização de testes ou ensaios e fazer com que se utilizem componentes mais baratos, normalmente com uma inerente menor fiabilidade (embora não necessáriamente).

Regra geral, verifica-se que a utilização de componentes mais baratos ou o recurso a pequenas amostragens podem significar poupanças a curto prazo, mas normalmente resultam em custos superiores a longo prazo, que normalmente se traduzem em indemnizações ao abrigo de garantias ou à perda de confiança por parte dos clientes. Deve assim haver um equilíbrio entre a fiabilidade, satisfação do cliente, vendas e características do produto. Podem-se apontar algumas razões que justificam o estudo da fiabilidade, tais como:

- Produção de componentes com um nível de fiabilidade óptimo, o que se traduz por mínimos valores do custo do ciclo de vida para o utilizador e ao mesmo tempo minimizando os custos para o fabricante sem comprometer a fiabilidade e qualidade do produto;
- Produção de componentes para uma vida expectável, baixando a probabilidade de ocorrência de avaria antes do tempo de missão, mas sem que se produza algo que perdurará muito mais tempo do que o necessário;
- Evitar avarias catastróficas. Veja-se o exemplo da indústria aeronáutica e aeroespacial onde o estudo da fiabilidade é de extrema importância e tem reflexos na segurança deste tipo de transporte;
- Reflectir as promessas ou requisitos que os produtos devem possuir no que respeita a valores anunciados. Um cliente não satisfeito poderá ter consequências desastrosas (dependendo da importância desse cliente relativamente ao fornecedor). Por curiosidade, pode-se referir alguns dados estatísticos que mostram que um cliente satisfeito pode indicar um produto a 8 pessoas enquanto um cliente insatisfeito contará em média a 22 pessoas a sua insatisfação (Pallerosi, 2006);
- Aplicações críticas, onde a fiabilidade é factor chave.

A implementação de um programa de fiabilidade apresenta algumas vantagens que podem ser descritas nos seguintes pontos:

- Tempo de "*burn-in*"[1] óptimo;
- Período de garantia óptimo e estimativa dos seus custos, redução de custos de garantia ou aumento do prazo de garantia para o mesmo custo;
- Tempo óptimo de substituição preventiva de componentes em sistemas reparáveis;
- Requisitos de sobressalentes;

[1] "*Burn-in*" refere-se a uma técnica utilizada por alguns fabricantes, onde os componentes ou sistemas são sujeitos ou colocados a funcionar sob determinadas condições mais severas do que as normais de funcionamento, a fim de verificar possíveis defeitos ou fraquezas dos mesmos, garantindo assim que aquando da sua entrada em funcionamento este tipo de falhas não se verifique. Pode-se inserir numa política de qualidade, verificando-se a sua aplicabilidade fundamentalmente em componentes eléctricos e electrónicos. Esta técnica terá mais valor se for suportada por modelos que permitam fazer uma extrapolação das condições de ensaio para as condições reais de funcionamento.

- Melhor informação acerca dos tipos de avarias (que podem ajudar a fase de projecto) e os esforços necessários em investigação e desenvolvimento para minimizar essas avarias;
- Estabelecimento dos tempos para a avaria esperados e preparação para a ocorrência das mesmas;
- Estudos dos efeitos da idade, duração da missão e aplicação de níveis de carga na fiabilidade;
- Comparação de dois ou mais projectos do ponto de vista da fiabilidade;
- Avaliação de redundâncias (projecto) e estimativas do seu número para se alcançar determinada fiabilidade;
- Guia para tomada de decisões de acções correctivas para minimizar as avarias, reduzir os tempos de manutenção e reparação e evitar sub ou sobredimensionamentos;
- Guia de ajuda para estabelecer as boas práticas de inspecção da qualidade;
- Optimização do objectivo de fiabilidade no projecto de produtos para reduzir custos;
- Capacidade de condução de estudos de manutibilidade, disponibilidade, custos, operacionalidade, etc…;
- Capacidade de avaliar fornecedores do ponto de vista da fiabilidade;
- Promoção das vendas com base em índices de fiabilidade dos produtos;
- Aumentar a satisfação do cliente, com o consequente aumento das vendas;
- Promoção da imagem e reputação da empresa.

Se houver um deficiente sistema de informação sobre avarias, o fabricante nunca irá saber realmente o grau de satisfação dos seus produtos em funcionamento. Na eventualidade dos mesmos se encontrarem a operar satisfatoriamente também se pode ter a situação inversa, ou seja, ter custos de projecto e fabrico desnecessários face à fiabilidade requerida, reduzindo os lucros. Devido ao crescente aumento da complexidade dos equipamentos e adição de novos componentes, os produtos com fiabilidades actualmente aceitáveis necessitam de ser monitorizados para se analisar a evolução desta característica.

2.3.1 – Fiabilidade e Qualidade

Muitas vezes os termos “qualidade” e “fiabilidade” são aplicados como se fossem semelhantes. No entanto, existe uma diferença fundamental entre estes dois conceitos

pois, enquanto a fiabilidade se refere ao desempenho de um bem durante a sua vida inteira, o controlo de qualidade está relacionado com o desempenho desse bem num determinado tempo particular e específico, sendo este momento normalmente estabelecido durante um processo de fabrico.

Tal como referido na própria definição, a fiabilidade prevê a probabilidade dos componentes, sistemas e equipamentos funcionarem sem avarias durante determinados períodos de tempo ao longo da sua vida, desde a concepção até ao abate ou desmantelamento.

O controlo de qualidade situa-se num momento concreto, embora também importante, assegurando a conformidade com as especificações ou certificando que os produtos são testados e inspeccionados correctamente.

De facto, existem algumas diferenças entre o controlo de qualidade tradicional e a fiabilidade, nomeadamente:

- A fiabilidade pode ter por objectivo analisar a taxa de avarias durante um longo período de duração (tempo, ciclos, quilómetros, etc), enquanto o controlo de qualidade focaliza a percentagem de bens analisados que se encontra fora de especificação (ou com defeito), num determinado instante do processo de fabrico, montagem ou teste;
- A fiabilidade actua em qualquer instante da vida do bem, desde a sua concepção até à fase de abate ou desmantelamento, enquanto o controlo de qualidade actua fundamentalmente durante a fase de fabrico;
- A fiabilidade visa aplicar conceitos e metodologias de forma a obter sucesso no que diz respeito à sobrevivência dos bens, enquanto o controlo de qualidade tem o objectivo de converter de forma correcta desenhos e especificações em produtos;
- A fiabilidade deve garantir um bom produto, de acordo com a sua utilização, enquanto o controlo de qualidade parte do pressuposto que não existe degradação durante as fases de fabrico, montagem e teste;
- O controlo de qualidade assume uma uniformidade dos bens produzidos, dentro das especificações (com custos de análise aceitáveis para os consumidores).

Para Ferreira (1998), chamamos qualidade dum produto à sua conformidade com uma especificação à saída de fábrica (t=0) e fiabilidade à sua capacidade de mantê-la durante a sua "vida de funcionamento".

Neste sentido, poder-se-á também afirmar que a fiabilidade é a extensão da qualidade ao longo do tempo. Nesta perspectiva, e de acordo com Pallerosi (2006), o controlo de qualidade pode ser caracterizado em quatro tipos:

- Qualidade dimensional (materiais, dimensões, pesos, etc);
- Qualidade operacional (funcionalidade, durabilidade, possibilidade de reparação, condições de praticabilidade, custos operacionais e obsolescência);
- **Qualidade temporal** (fiabilidade, manutibilidade e disponibilidade);
- Qualidade comercial (preço de venda, condições de pagamento, assistência técnica, imagem do produto, prazo de entrega, armazenamento, transporte e comercialização).

O tipo de qualidade que caracteriza a vida do bem, não apenas no instante inicial da sua entrada em serviço, é a qualidade temporal, uma vez que trata tipos de acontecimentos como avarias, reparações e utilização efectiva. A qualidade temporal refere-se a determinados atributos mensuráveis como a probabilidade de sobrevivência (ou fiabilidade) (R), ou a sua complementar probabilidade de falha (F), probabilidade de reparação ou recolocação em serviço (ou manutibilidade) (M) e probabilidade de uso efectivo (ou disponibilidade) (A).

Todos estes factores são influenciados por acontecimentos indesejáveis, como por exemplo:

- Avarias significativas na fase inicial da vida operacional (muitas vezes denominadas avarias infantis);
- Exagerados tempos de paragem para reparação;
- Aumento dos custos de manutenção;
- Necessidade de redundâncias;
- Operação ou segurança comprometidas;
- Etc.

Devem-se ter sempre em atenção alguns aspectos importantes relacionados com este tipo de análises, tais como: ter a noção que qualquer probabilidade se relaciona sempre com um determinado nível de confiança, definir correctamente o objecto em análise (seus sistemas e componentes), o que se entende por bom funcionamento, quais as condições operacionais (ambientais, de utilização e de manutenção), assim como o período de tempo estudado.

2.3.2 – Bens reparáveis e bens não reparáveis

Quando se fala de análises de fiabilidade, um tema bastante importante e que convem definir à partida é a noção de bem reparável e de bem não reparável. Um bem diz-se reparável se após a sua avaria é possível repor as condições que permitem continuar a cumprir a sua função, tal como inicialmente especificado. Para isso, procede-se à sua reparação (substituição de componentes, ajustamento, lubrificação, aperto, etc.). Um bem diz-se não reparável, ou descartável, se após a avaria se procede à sua substituição por um outro bem idêntico (novo).

Em traços gerais, se um bem é descartável (como por exemplo uma lâmpada ou um transístor), ao determinar a sua fiabilidade teremos que ter em conta que apenas uma avaria pode ocorrer. Valores de vida como a vida média ou o tempo médio até à avaria (MTTF) são características que podem ser usadas para este tipo de bens. Quando um componente avaria num sistema não reparável (com componentes em série), o próprio sistema normalmente fica em falha e a sua fiabilidade é uma função no tempo da primeira avaria do componente (O'Connor, 1999). Quando nos referimos a bens não reparáveis, a probabilidade instantânea da sua primeira e única avaria denomina-se função de risco (*hazard function*). A expressão "taxa de avarias" só se deve aplicar a bens reparáveis, uma vez que só num sistema reparável os componentes irão contribuir para a taxa de avarias do sistema (O'Connor, 1999).

Quando se trata de bens reparáveis, o tempo necessário à sua reparação e recolocação em serviço é muito importante, condicionando a disponibilidade dos equipamentos em maior ou menor grau. Neste caso, considera-se o tempo médio entre avarias (MTBF) dos bens, assim como o seu tempo médio de reparação (MTTR), sendo estes alguns dos parâmetros importantes no estudo da sua disponibilidade.

Os trabalhos de reparação e recolocação em serviço podem ser executados no próprio local onde o equipamento se encontra, ou, em determinadas situações, ser necessário remover o bem avariado e proceder à sua reparação em oficina. Nos casos em que esta segunda condição se verifica, se procedermos à substituição do bem avariado por um outro idêntico (que se encontrava em armazém), realizando-se em paralelo a reparação do primeiro, o bem designa-se por "rotável".

Normalmente, quando se referem bens reparáveis estamo-nos a referir a sistemas, enquanto os componentes são regra geral definidos como bens não reparáveis[2]. Curiosamente alguns bens podem ser considerados como reparáveis ou não reparáveis, como é o exemplo de um míssil que pode ser um sistema reparável enquanto se encontra armazenado (sujeito a testes periódicos) mas quando lançado se torna um sistema não reparável.

Para este tipo de sistema, as análises de fiabilidade têm que ser efectuados distintamente para cada um dos estados. Outras considerações, como o custo, também podem definir se um bem é considerado reparável ou não reparável, como por exemplo uma placa electrónica de televisão, onde ser ou não ser reparável poderá depender do seu custo de reparação (O'Connor, 1999).

A maior parte dos bens possui características de vida que podem ser ilustradas graficamente. Um exemplo dessas representações é a sobejamente conhecida curva da banheira. A Figura 2.2 corresponde a uma curva típica da variação da taxa de avarias (avarias por unidade de tempo) no tempo (horas, ciclos, quilómetros, etc.), para bens reparáveis, onde se podem distinguir três fases distintas. A duração de cada fase, assim como o seu comportamento, variam de acordo com o tipo de bem estudado.

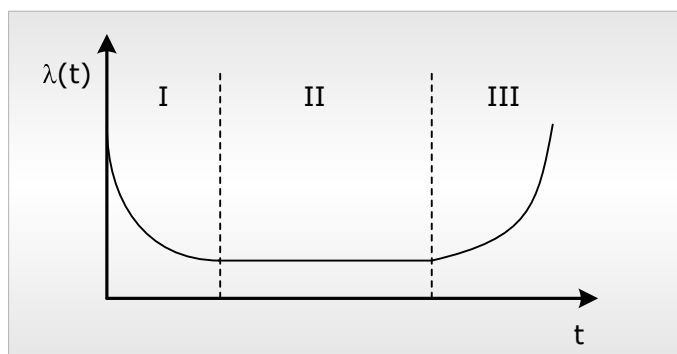



Figura 2.2 – Curva da banheira típica

A maioria dos bens começa a sua vida com uma taxa de avarias mais elevada devido a certos factores, como por exemplo defeitos de fabrico, má montagem ou deficiente controlo de qualidade de alguns dos seus componentes. Nesta fase, denominada período

---

[2] Eventualmente, em alguns casos, existirão componentes que após a avaria poderão ser recondicionados e colocados novamente em operação, sendo nessa perspectiva considerados bens reparáveis.

de infantil, os bens apresentam uma taxa de avarias decrescente, uma vez que os problemas iniciais são gradualmente identificados e corrigidos.

Posteriormente, esta taxa de avarias estabiliza num valor aproximadamente constante durante o período de vida útil, onde as avarias ocorrem aleatoriamente, e de forma inesperada ou imprevista.

A última fase, designada fase de desgaste ou envelhecimento, é caracterizada por um aumento rápido da taxa de avarias no tempo devido a desgaste, perda de características importantes (elasticidade, solubilidade, etc…) ou degeneração das mesmas. De certo modo, podemos fazer uma analogia com a taxa de mortalidade para os humanos, de acordo com o seu tempo expectável de vida.

No entanto, o modelo apresentado na figura anterior não é único, podendo fundamentalmente ser utilizado para demonstrar o comportamento da taxa de avarias ao longo do tempo dos bens reparáveis que incluem tecnologias variadas, podendo ser considerada como uma linha de tendência resultante das diferentes distribuições de falhas dos componentes de um sistema (Monchy, 2003).

John Moubray (1997) refere esta relação entre a avaria e a idade de um bem, mostrando a evolução deste conceito ao longo do tempo e subdividindo-o em três gerações temporais.

Na primeira geração a visão era de que a avaria se relacionava exclusivamente com a idade, ou seja, só ao fim de um determinado período de operação é que se manifestariam fenómenos de falha.

Ao se considerarem as avarias infantis surgiu então a designação de "curva da banheira", tal como apresentado na Figura 2.2, sendo esta abordagem designada por Moubray como segunda geração.

A terceira geração mostra que na prática se podem obter seis padrões de comportamento das avarias no tempo, tal como ilustrado na Figura 2.3.

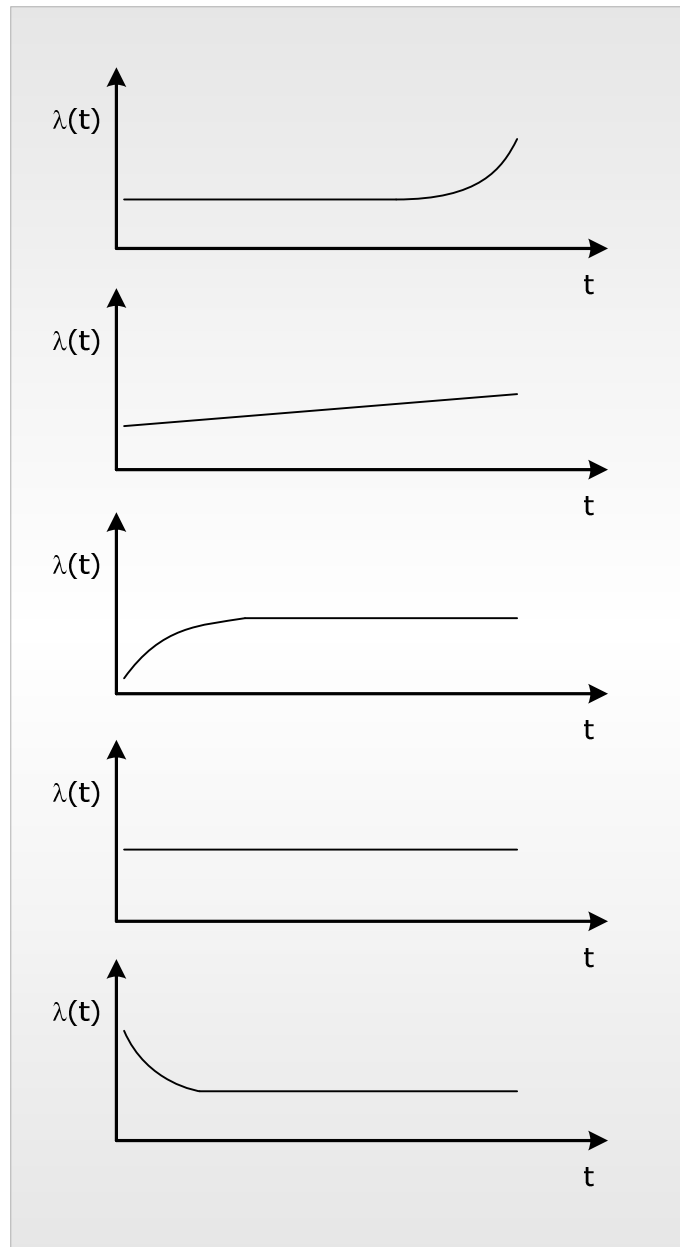



Figura 2.3 – Padrões de representação da taxa de avarias

Uma outra questão importante que deve ser referida tem a ver com a dependência ou independência dos acontecimentos. Assim, dois acontecimentos são independentes se a ocorrência de um não afecta a probabilidade de ocorrência do outro. Esta diferenciação é muito importante quando se analisam questões como a avaria de bens, e onde a dependência pode ter um papel muito importante no método e nos resultados obtidos.

2.3.3 – Fiabilidade Humana

Outro componente de grande importância na área da fiabilidade e gestão do risco diz respeito ao factor humano e organizacional que, devido à sua especificidade, ao grau de complexidade e por se afastar um pouco dos objectivos deste trabalho, não será abordado detalhadamente, embora mereça ser discutido por especialistas nesta área quando se estudam processos onde a sua influência é determinante.

Trata-se de uma matéria actual (alvo de investigação recente), na tentativa de mudar a ideia instalada de que “*errar é humano*”. O erro humano pode ser quantificado pela sua frequência, definida através do número de erros cometidos por um indivíduo em “n” solicitações ou pelo número de erros cometidos durante um determinado período de observação. Trata-se de perceber os erros humanos, suas causas e consequências, com o objectivo de reduzir a sua ocorrência até limites aceitáveis.

De acordo com alguns autores, o erro humano tem um papel fundamental na ocorrência de acidentes em sistemas de segurança críticos, tais como na aviação, sistemas ferroviários ou instalações nucleares (Reason, 1990).

De facto, e de um modo simplista, a fiabilidade humana (HRA = *Human Reliability Analysis*) pode ser analisada num paralelismo com a lógica das análises de fiabilidade dos equipamentos, podendo os erros ser classificados, quantificados e matematicamente analisados por meio de uma adequada distribuição estatística. Ao contrário da maioria dos equipamentos, que sofrem uma degradação ao longo do tempo no cumprimento de uma missão, os erros humanos podem ser reduzidos tendo em conta alguns factores (Pallerosi, 2007), como:

- Aptidão;
- Treino;
- Experiência;
- Idoneidade.

Ainda de acordo com o mesmo autor, no quotidiano das empresas é comum a ocorrência de erros (falhas humanas), devido a várias causas e motivos, sendo 75% dos mesmos alocados às seguintes áreas de actuação:

- Inspecção (25%);
- Manutenção (22%);
- Operação (15%);

- Gestão (13%).

As causas apontadas anteriormente têm fundamentalmente a ver com falta de conhecimento (40%), procedimentos técnicos incorrectos (20%) e causas pessoais[3] (15%). Os restantes 25% das causas são indirectas e têm a ver com o projecto (11%), com os materiais (8%), com causas ambientais (5%) e outras (1%).

Os erros humanos também podem ser agrupados em cinco categorias, nomeadamente (Assis, 2004):

- Erro de omissão – não executar a operação que estava inicialmente programada;
- Erro de execução – executar a tarefa, mas não da forma prevista;
- Erro de derivação – introdução de uma acção não prevista;
- Erro de sequência – a operação é executada, mas não no momento que devia ser;
- Erro de atraso – a tarefa é executada, mas tardiamente.

A fiabilidade humana pode ser avaliada em duas fases: a fase de aprendizagem (taxa de erros decrescente) e a fase de execução (erros aleatórios).

Presentemente existem várias metodologias sobre esta temática. A quantificação dos erros humanos pode ser efectuada com recurso a metodologias mais simples, como a TESEO (*Technique for Empirical Simulation of Errors in Operations*) ou a HEART (*Human Error Asessment and Reduction Technique*), ou através de métodos mais complexos como o THERP (*Technique for Human Error Rate Prediction*), o CREAM (*Cognitive Reliability and Error Analysis*), o ASEP (*Accident Sequence Evaluation Program*) ou o MPPS (*Maintenance Personnel Performance Simulation*) (Hollnagel, 1998).

Tal como já referido anteriormente, este factor designado por fiabilidade humana, e consequentemente o estudo de uma qualquer metodologia nesta área, não fazem parte dos objectivos do presente trabalho, pretendendo-se apenas fazer referência a este assunto, muitas vezes de vital importância na gestão do risco.

[3] As referidas causas pessoais, tal como o próprio nome indica, englobam aspectos da vida pessoal que terão reflexo no desempenho de um determinado indivíduo durante o período de trabalho. A título de exemplo podem ser referidos problemas familiares ou de saúde ou outro qualquer motivo de preocupação que é transportado para o ambiente de trabalho.

2.3.4 – Avarias devido a causa comum

A redução da ocorrência de potenciais avarias de um bem assenta fundamentalmente em três princípios, nomeadamente, no aumento da fiabilidade dos seus componentes, no uso de sensores (que permitem obter a informação antecipada sobre uma potencial avaria) e na utilização de redundâncias activas ou passivas (utilizando sensores-comutadores).

Hoje em dia, devido ao elevado desenvolvimento tecnológico, restrições de aquisição ou aos custos elevados, torna-se difícil em muitos casos aumentar ou melhorar a fiabilidade dos componentes. Por outro lado, a aplicação de sensores muitas vezes não é fisicamente possível de realizar, e quando exequível, se por um lado normalmente comporta custos elevados, por outro não melhora a fiabilidade em termos individuais (componentes), reflectindo-se essa melhoria apenas ao nível do sistema. Deve-se assim dar particular importância à utilização de redundâncias quando se analisam bens de alto risco, possibilitando alcançar maiores valores de fiabilidade para os sistemas.

No entanto, a ocorrência de avarias denominadas de causa comum (CCF = *Common Cause Failures*) pode provocar a avaria de componentes, sensores e eventualmente redundâncias, anulando por vezes evidentes vantagens de concepção dos sistemas.

As avarias de causa comum correspondem a avarias em múltiplos componentes que ocorrem devido a uma causa única que é comum a todos eles. No estudo de Volkanovski *et al* (2009) apontam-se como exemplos de avarias de causa comum a ocorrência de condições atmosféricas severas ou tremores de terra numa determinada região e seus efeitos sobre várias linhas de um sistema de transmissão de energia.

Para exemplificar melhor este tipo de avarias e a sua importância no contexto de análises de fiabilidade na indústria, pode-se dar o exemplo de uma linha de produção onde seja necessário o funcionamento de um sistema de ar comprimido para alimentação e controlo dessa linha. Se for considerada uma avaria na alimentação da energia eléctrica, verifica-se que esta situação põe em causa o funcionamento de todo o sistema, independentemente de poder haver compressores em redundância ou sensores que sinalizem a avaria, sendo assim considerada uma avaria de causa comum.

A terminologia sobre avarias de causa comum tem sofrido alterações ao longo dos anos, tendo começado por se confundir este tema com falhas de modo comum[4] (modo de falha). Com a introdução do termo "avaria dependente" estes dois conceitos foram fundidos. No entanto, podem-se considerar falhas de modo comum como um subconjunto das avarias de causa comum.

Em instalações industriais de risco elevado, como é o caso de centrais nucleares, refinarias ou centrais termoeléctricas, torna-se fundamental conhecer as potenciais avarias de causa comum e sistematizar a sua prevenção. Estas avarias são na maior parte dos casos resultado de falhas de concepção e gestão, e noutras situações resultantes de falhas técnicas, reduzindo a disponibilidade dos sistemas.

A prevenção das avarias de causa comum é normalmente muito importante em situações que envolvam a segurança de uma instalação. Para sistemas altamente redundantes, este tipo de avarias pode ser a razão principal de avaria dos mesmos. **De que adianta ter um sistema com uma fiabilidade elevada, resultante da utilização de componentes redundantes, se existir uma causa comum de avaria a todos os seus componentes?**

Pode-se afirmar que as principais fontes de avaria de causa comum são relativas à engenharia e à operação, podendo ser repartidas da seguinte forma (Pallerosi, 2007b):

<u>Engenharia – Projecto</u>

- Falhas de concepção (dependências, protecções inadequadas, erros de dimensionamento, etc.);
- Falhas funcionais (erros de lógica, controlos inadequados, medições inadequadas, etc.).

<u>Engenharia – Construção</u>

- Falhas de fabrico (controlo de qualidade, inspecções e testes inadequados, etc.);
- Falhas de instalação (controlo de qualidade, inspecções e testes inadequados, inicio de operação mal conduzido, etc.).

<u>Operação – Projecto</u>

[4] De salientar que o modo de falha se refere à maneira pela qual é verificada a incapacidade de um bem para cumprir uma função requerida enquanto a causa se refere à razão que origina a avaria (NP EN 13306, 2007). Neste sentido é desaconselhada a utilização de "modo de avaria".

- Falhas de concepção (reparações e testes imperfeitos, calibrações e instruções incorrectas, supervisão deficiente, etc.);
- Falhas funcionais (erros dos operadores ou de comunicação, instruções incorrectas, supervisão deficiente, etc.).

Operação – Construção

- Falhas devido a valores extremos (temperatura, pressão, humidade, tensão, etc.);
- Falhas devido a acontecimentos ambientais (vento, terramoto, explosão, inundação, agentes químicos, etc.).

Apontada a importância deste tema, as atenções devem ser dirigidas para a prevenção contra a ocorrência de avarias de causa comum, desde a fase de projecto até à operação efectiva do equipamento.

Os procedimentos para minimizar as avarias de causa comum passam por questões técnicas e de gestão, nomeadamente:

- Gestão – A nível de projecto procedendo a especificações e ao controlo e revisões ao projecto. Na execução, exercendo controlo na construção e na montagem. Durante a operação, tendo um controlo operacional, uma boa gestão da manutenção e conhecendo valores de disponibilidade e de fiabilidade;
- Técnicas – Na especificação de avarias seguras, protecção, interfaces operacionais, redundâncias, simplicidade e diversidade funcional. Ter um controlo de qualidade seguindo as normas de construção, inspecção e arranque da instalação, assim como elaborando instruções de operação. Em termos operacionais, produzir instruções para operar e para efectuar testes e tendo especial atenção à gestão da manutenção.

Nesta área das CCF muitos trabalhos científicos têm sido desenvolvidos. A título de exemplo refira-se alguns estudos mais generalistas, onde se pretende uma optimização da fiabilidade dos sistemas na presença de avarias de causa comum (Ramirez-Marquez & Coit, 2007), ou casos mais específicos que passam por exemplo pela verificação das limitações impostas pelas avarias de causa comum na análise de fiabilidade de um sistema de corte de um reactor através de uma Árvore de Falhas (Kumar *et al*, 2005), ou ainda no cálculo de incertezas associadas às taxas das avarias de causa comum (Vaurio, 2005) (Vaurio, 2002).

Aparecem também alguns trabalhos sobre a estimativa dos parâmetros das avarias de causa comum baseados em testes periódicos (Lundteigen & Rausand, 2007) (Barros *et al*, 2009) ou estimativa das probabilidades de ocorrência dessas avarias quando se efectuam testes mistos aos componentes (Kang, 2009) ou quando se utiliza a análise de Árvore de Falhas (FTA) (Vaurio, 2003). Pode ser igualmente analisada uma metodologia interessante proposta por Vaurio (2007) onde se combina a informação operacional de várias instalações para estimar as taxas para as avarias de causa comum de uma instalação tipo.

2.3.5 – Modelos de fiabilidade

Em termos gerais podem-se considerar dois tipos fundamentais de modelos de fiabilidade, os determinísticos e os estatísticos (Pereira, 1996).

Os modelos determinísticos são modelos baseados nas leis de degradação física dos componentes ou sistemas sujeitos a avaria e são aplicados a sistemas reparáveis que seguem um Processo de Poisson Não Homogéneo (NHPP). É importante conhecer-se o que dá início ao processo, que condições ambientais o podem acelerar (ou potenciam o seu desenvolvimento), e como estas condições conduzem à avaria de um dado componente. Também há que controlar as formas pelas quais se consegue parar, ou normalmente diminuir a taxa de progressão dos efeitos associados. Com base no conhecimento do processo de deterioração dominante e da respectiva taxa de degradação, podem-se fazer previsões sobre a vida do bem analisado. A aplicação deste tipo de modelos a certos componentes pode prever o seu comportamento, com uma margem de erro relativamente pequena, tornando-se mais difícil quando se trata de equipamentos ou sistemas complexos. Nestes casos não é possível definir qual o processo de deterioração determinante, e a aplicação destes modelos também não permite o tratamento simultâneo de vários processos, salvo se houver um modo de avaria bem definido e predominante que se sobreponha a todos os outros (Pereira, 1996).

Os modelos estatísticos são modelos de fiabilidade que recorrem ao conhecimento de situações ocorridas no passado com um determinado bem (ou com bens semelhantes) para inferir sobre a condição futura desse bem, quer seja através do ajustamento a uma distribuição de tipo previamente definido ou através do cálculo de uma função própria caracterizadora da fiabilidade prevista, designando-se por modelos paramétricos e

modelos não paramétricos, respectivamente. As variáveis podem ser discretas ou continuas e a cada uma delas pode ajustar-se a distribuição que for mais conveniente. O ajustamento de uma dada distribuição aos dados de vida de um componente deverá pressupor que o funcionamento desse componente não é afectado pela avaria de outro qualquer componente do sistema.

2.3.6 – Estimativas da Fiabilidade

Em fiabilidade, o resultado de uma análise de dados de vida traduz sempre uma previsão ou estimativa, quer se trate de prever o valor da probabilidade de avaria, probabilidade de sucesso, vida média ou outros parâmetros de uma determinada distribuição.

Assim, a fiabilidade, como ramo da engenharia, tem como objectivo estimar valores de forma apurada, com base na análise dos dados de vida dos bens. Tal como referido anteriormente, estas estimativas podem basear-se em amostragens.

Para ilustrar as bases dos testes de amostragem, pode-se recorrer ao exemplo clássico de bolas brancas e bolas pretas, cujo objectivo é estimar a percentagem de cada um destes tipos de bolas que se encontram num determinado universo. Imaginemos uma piscina gigante cheia de bolas e comecemos por retirar uma pequena amostra de 10 unidades, contando-se quantas bolas pretas se encontram nessa mesma amostra. Imaginemos que contámos 4 bolas pretas, ou seja, com base nesta amostra estima-se em 40% o número de bolas pretas dentro da referida piscina. Se repetirmos, mas agora com uma amostra de 1000 bolas poderemos obter, por exemplo, quantidades de bolas pretas entre 445 e 495, correspondendo a estimativas entre 44,5% e 49,5%, o que traduz uma variação da estimativa muito menor. Assim, podemos afirmar que quanto maior for a quantidade da amostra mais apurada será a nossa estimativa. Desta forma, pode-se afirmar que a incerteza referente ao valor real do parâmetro a estimar é menor quando possuímos mais informação.

Esta questão da incerteza associada a um determinado cálculo de fiabilidade pode traduzir o resultado de dois tipos de incertezas; as que se relacionam com os dados analisados e as que reflectem as incertezas inerentes ao próprio modelo utilizado na determinação dos valores. Para um sistema, a variabilidade no cálculo de determinado parâmetro pode traduzir-se pela soma das várias incertezas parciais em jogo.

Muitas vezes, em alternativa a amostras ou ensaios, recorre-se a bases de dados existentes, onde constam alguns parâmetros fiabilisticos referentes a bens, cujos elementos foram compilados por determinada entidade ou organização. Temos como exemplo a OREDA (2002), dirigida a um sector específico da actividade industrial, cuja intenção passa por permitir a utilização de dados na avaliação e melhoria da segurança e fiabilidade nas indústrias de petróleo e gás (exploração e produção).

O projecto OREDA foi iniciado em 1981 em cooperação com o *Norwegian Petroleum Directorate* cujo objectivo inicial era a recolha de informação fiabilistica de equipamentos de segurança. Em 1983, a organização envolveu um grupo de várias companhias petrolíferas e alargou o seu campo de recolha de dados a outros tipos de equipamentos. Apesar da cobertura ser fundamentalmente sobre instalações *offshore*, algumas instalações *onshore* de petróleo e gás também foram consideradas.

O objectivo principal do projecto OREDA é contribuir para uma melhoria da segurança e eficácia de custos do projecto e operação de instalações de petróleo e gás através da recolha e análise de informação sobre a manutenção e operação, criando uma base de dados fiabilisticos de alta qualidade, assim como a troca de tecnologia RAMS entre as empresas participantes. Na publicação anteriormente referida está representado o período de análise entre 1993 e o ano 2000.

Outros documentos podem ser referidos quando se pretende estimar a fiabilidade de bens. Por exemplo, para componentes electrónicos pode-se referir o MIL-HDBK-217F (1991) e a TELCORDIA SR-332 (BELLCORE TR-332) (2006). Para componentes mecânicos (vedantes, molas, rolamentos, engrenagens, válvulas, etc.) pode-se indicar a publicação da NSWC-09 (2009).

Uma outra forma de se prever a fiabilidade de um bem é através de ensaios. Basicamente, os resultados obtidos nos ensaios, quer sejam acelerados ou não, visam principalmente definir os parâmetros de fiabilidade que poderão constar nos contratos de compra e venda, incorporar os requisitos de fiabilidade nas especificações gerais do produto ou confirmar informações baseadas em ensaios efectuados por terceiros. Os ensaios podem ser classificados segundo vários critérios, fundamentalmente:

- Quanto ao local da prova (ensaios de laboratório (*Lab-tests*) ou ensaios de campo (*Field-tests*));
- Quanto ao tipo de acontecimento (avaria, suspensão, interrupção, recolocação);

- Quanto às regras de substituição (sem substituição, com substituição ou com reparação);
- Quanto às regras de conclusão dos ensaios (ensaios completos ou ensaios censurados).

A Figura 2.4 mostra um esquema referente às variáveis a ter em conta nos ensaios para determinação da fiabilidade.

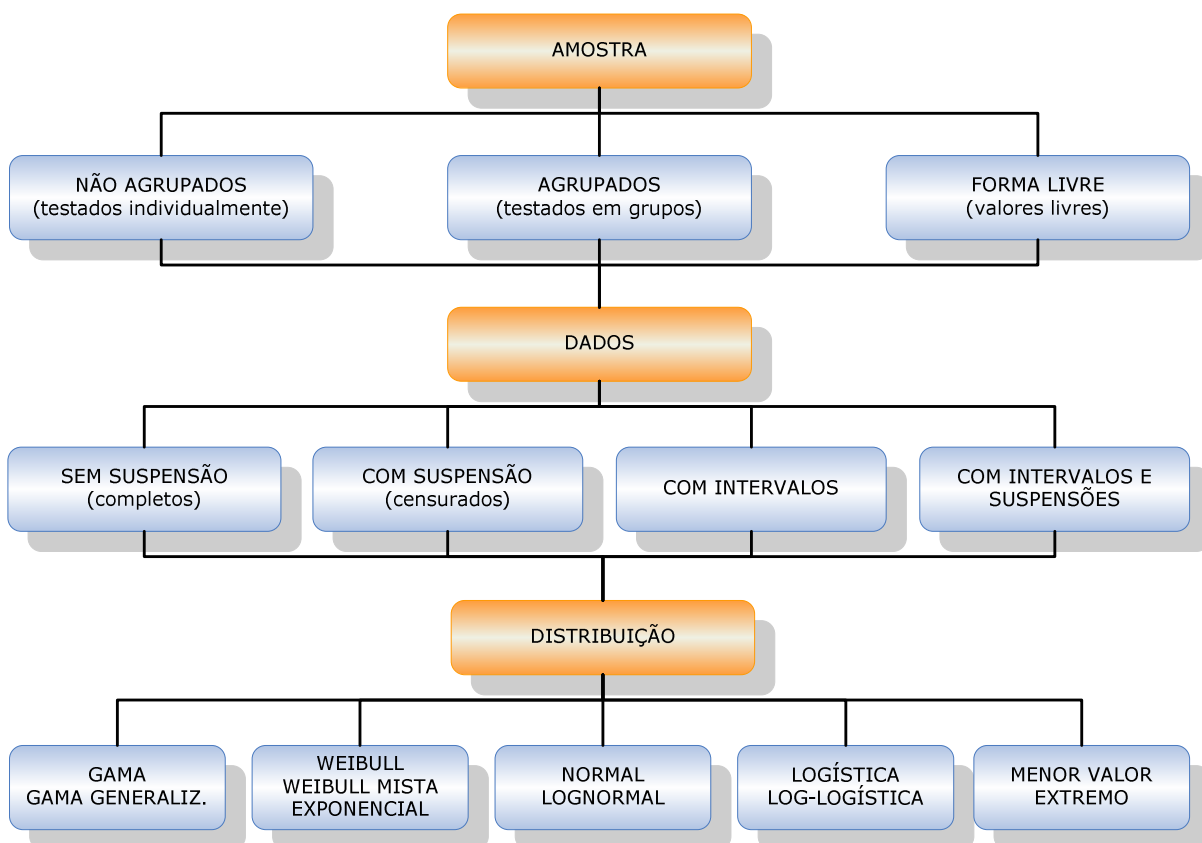



Figura 2.4 – Metodologia para ensaios de fiabilidade
[Fonte: Pallerosi (2006)]

O conhecimento da fiabilidade de um bem durante as fases de desenvolvimento, fabrico, instalação e operação, pode ser obtido através de três meios diferentes de ensaios, nomeadamente:

- Ensaios normais;
- Ensaios acelerados (ALT = *Accelerated Life Tests*);
- Ensaios altamente acelerados (HALT = *High Accelerated Life Tests*).

A Figura 2.5 mostra as principais características das amostras, as durações e os tipos de aceleração correspondentes.

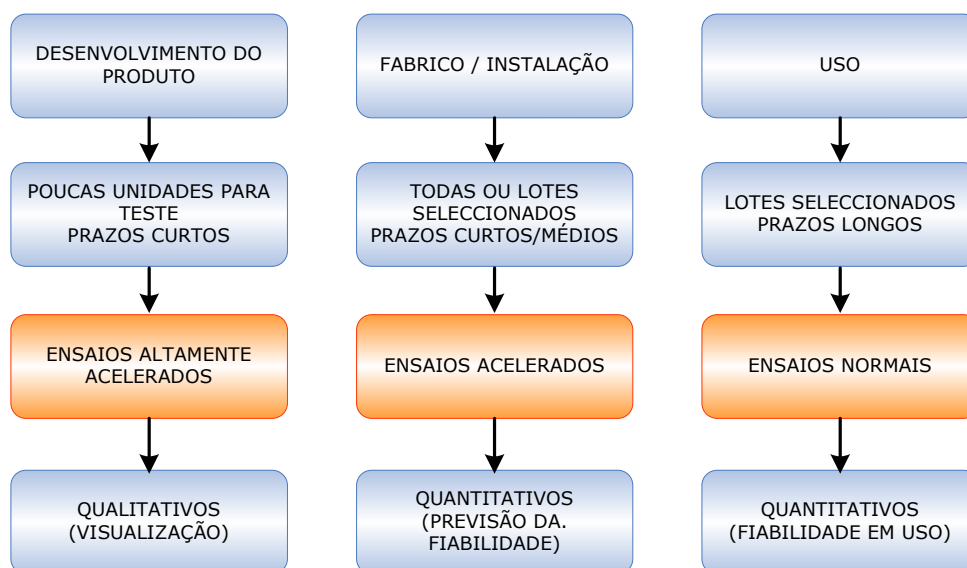



Figura 2.5 – Aplicações típicas de ensaios
[Fonte: Pallerosi (2007c)]

O objectivo dos ensaios altamente acelerados (HALT) é o de visualizar prováveis modos de falha e efeitos de forma a corrigi-los, ou seja, basicamente demonstrar como o produto se degradaria com o uso. Este tipo de ensaios promove uma alta degradação nas amostras, sendo por isso algumas vezes referenciados como testes de "elefante" ou de "tortura".

Os ensaios acelerados (ALT) assentam em duas condições básicas (Pallerosi, 2007c):

1. As solicitações aplicadas são maiores que as normalmente exigidas na utilização normal do produto;
2. As solicitações não devem alterar significativamente os modos, os efeitos e a criticidade das falhas.

Os objectivos dos ensaios acelerados são:

- Permitir o rápido desenvolvimento de novos produtos e tecnologias;
- Testar e adoptar rapidamente novas tecnologias e produtos disponíveis no mercado;
- Testar produtos mais complexos, com mais componentes (com maior probabilidade de avaria);

- Satisfazer as expectativas dos consumidores (exigência de melhores requisitos).

As acções (ou etapas) que fazem parte de um processo de ensaios acelerados assentam inicialmente na escolha do tipo de solicitação (stress), com a selecção de pontos sensíveis, meios, leis de degradação, etc., passando posteriormente pela escolha do tipo de aceleração (taxa de avarias ou duração) e pela determinação das probabilidades de falha (tipo de ensaio e parâmetros da distribuição estatística), sendo por fim calculados os parâmetros da aceleração (Pallerosi, 2007c).

Recentemente tem surgido a publicação de alguns trabalhos científicos na área dos ensaios acelerados, mostrando assim a sua actualidade e a sua importância no contexto das análises de fiabilidade. Os ensaios acelerados têm servido para prever a fiabilidade de um bem usando, por exemplo, incrementos sequenciais dos esforços aplicados durante o teste (Fard & Li, 2009). Têm também sido aplicados em estudos experimentais para determinação da fiabilidade e comportamento de componentes muito concretos relacionados com diferenciadas áreas da engenharia, como válvulas de solenóide hidráulicas (Angadi *et al*, 2009), vedantes em material EPDM (Placek *et al*, 2009), micro-juntas (Khatibi *et al*, 2008), asfalto (Yeo *et al*, 2008), células de combustível (Pei *et al*, 2008), componentes estruturais no campo aeroespacial (Ozsoy *et al*, 2008) e aeronáutico (Charruau *et al*, 2006) ou até mesmo no campo alimentar, como por exemplo para verificar o comportamento do azeite quando armazenado (García-García *et al*, 2008).

Também têm servido para prever o comportamento de vida de alguns elementos, em conjunto com outras técnicas como as redes neuronais (Freitag *et al*, 2009), ou a inferência Bayesiana (assumindo a distribuição de Weibull e utilizando Cadeias de Markov e simulação de Monte Carlo) (Dorp & Mazzuchi, 2005).

Encontram-se também alguns estudos referentes a testes acelerados de corrosão, que poderão servir para avaliar este modo de degradação em elementos estruturais, como por exemplo aço inoxidável sujeito a ambientes marinhos (Kosaki, 2008) ou fibras de carbono reforçadas sob acção simultânea de temperatura e água do mar (Nakada & Miyano, 2008). Relativamente ao tema dos ensaios acelerados poder-se-ia ir mais além, mas como o mesmo não se encontra especificado como o objectivo principal do presente trabalho, ficam apenas referenciadas algumas das considerações anteriormente apresentadas, julgadas pertinentes.

2.3.7 – Conceitos relacionados com a fiabilidade

Vejamos agora algumas funções e conceitos importantes quando se fala em estudos de fiabilidade.

2.3.7.1 – Função densidade de probabilidade de falha, fiabilidade e probabilidade acumulada de falha

A função densidade de probabilidade de falha é um poderoso instrumento de visualização de como as avarias ocorrem durante a vida de um bem e como elas estão estatisticamente distribuídas.

A função densidade de probabilidade de falha representa a função de probabilidade instantânea ou função mortalidade e traduz a quantidade de bens que estão a avariar num momento "t", por unidade de tempo, relativamente à população inicial e não está condicionada à quantidade de sobreviventes no instante anterior a "t", daí se designar também por probabilidade incondicional. Dá-nos a probabilidade do bem avariar exactamente no instante "t".

Esta informação pode servir para comparar produtos e verificar os diferentes comportamentos das falhas ao longo da sua vida. Este tipo de estudo pode servir, por exemplo, para estipular um prazo de garantia ou especificar uma vida média para um determinado bem.

Para variáveis aleatórias contínuas (tempo, quilómetros, ciclos, etc…) a probabilidade da variável aleatória pertencer a um dado intervalo corresponde à área sob a curva de variação da função densidade "f(t)" entre os extremos desse intervalo, ou seja:

$$P(t_a \leq t \leq t_b) = \int_{t_a}^{t_b} f(t).dt \qquad (2.1)$$

Se esta função for integrada entre o momento de entrada em funcionamento (t=0) e um momento genérico "t" (t<∞), obtemos a função de probabilidade acumulada de falha "F(t)", de acordo com a seguinte expressão:

$$F(t) = \int_0^t f(t).dt \qquad (\leq 1) \tag{2.2}$$

Para toda a vida do bem, a área abaixo da curva de variação da função densidade (densidade de probabilidade de falha) corresponde à sua totalidade, logo a probabilidade de falha no infinito, a que se refere uma curva de densidade de probabilidade entre zero e infinito, assume o valor 1 (100%). Em qualquer circunstância, depois de calculada a probabilidade de falha “F(t)”, a probabilidade de sucesso, ou função fiabilidade “R(t)”, pode ser facilmente determinada, uma vez que estas duas probabilidades são complementares.

$$R(t) + F(t) = 1 \tag{2.3}$$

Um exemplo de uma função densidade de probabilidade de falha, assim como a interpretação gráfica das funções probabilidade acumulada de falha e fiabilidade, encontra-se representado na Figura 2.6.

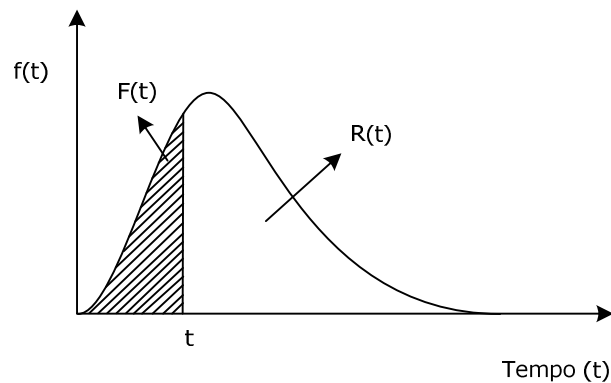



Figura 2.6 – Representação gráfica de uma função densidade de probabilidade de falha

A probabilidade de sucesso, ou fiabilidade, pode ser apresentada como a probabilidade do tempo correspondente à falha “t_f” ser superior ao tempo considerado no estudo “t”, ou seja:

$$R(t) = \Pr(t_f > t) \qquad 0 < t < \infty \tag{2.4}$$

Ou, tendo em consideração as expressões (2.2) e (2.3), a função fiabilidade pode ser representada pela seguinte expressão:

$$R(t) = \int_{t}^{\infty} f(t).dt \qquad (\leq 1) \tag{2.5}$$

Ao analisar-se a fiabilidade para uma grande diversidade de bens, verifica-se que alguns desses bens apresentam uma vida muito curta, enquanto outros possuem uma enorme longevidade (sem a ocorrência de avarias). Também para uma mesma duração da análise, existem casos em que as avarias podem ocorrer logo desde o início de operação, e situações em que as avarias só se verificam numa fase mais avançada, após decorrido um dado período do tempo. Assim, a função densidade de probabilidade de falha pode assumir diversas configurações, sendo esta variabilidade alvo de estudo mais detalhado em futuros parágrafos.

2.3.7.2 – Função de Risco. Taxa de avarias

De acordo com a vasta literatura existente na área da fiabilidade, e conforme os diversos pontos de vista dos autores sobre este assunto, constata-se que existe alguma confusão entre o conceito de função de risco e o de taxa de avarias. Basicamente, a grande diferença é que o conceito de taxa de avarias só se pode aplicar a bens reparáveis, quando considerados isoladamente.

A taxa de avarias está ligada a acontecimentos repetitivos (avarias), sendo o seu tempo de referência contado desde a entrada em funcionamento do bem até ao momento da análise. Por seu lado, a função de risco refere-se a um acontecimento único, sendo neste caso tido como referencial o tempo desde o último acontecimento. A função de risco “h(t)” é definida como uma probabilidade condicional, dado que a avaria não é verificada até ao tempo “t”, e pode matemáticamente ser expressa através da expressão 2.6.

$$h(t) = \lim_{\Delta t \to 0} \frac{P(t < tf \leq t + \Delta t \mid tf > t)}{\Delta t} \tag{2.6}$$

ou

$$h(t) = \frac{f(t)}{R(t)} \tag{2.7}$$

De acordo com as expressões (2.5) e (2.6), a fiabilidade também pode ser expressa através da seguinte expressão:

$$R(t) = e^{-\int_0^t h(t)dt} \qquad (2.8)$$

Assim:

$$h(t) = -\frac{d[\ln R(t)]}{dt} \qquad (2.9)$$

Deste modo, a função de risco pode ser interpretada como a diminuição relativa da fiabilidade por unidade de tempo. Traduz a taxa à qual os componentes estão a avariar por unidade de tempo, no momento "t+Δt", em relação ao número de sobreviventes no momento "t".

Quando se trata de bens reparáveis, sujeitos a ciclos de bom funcionamento interrompidos por estados de falha dos seus componentes, com as respectivas distribuições estatísticas, a taxa de avarias "λ(t)" do sistema relaciona-se com o processo estocástico que modela as avarias ao longo do tempo. Este pode ser considerado um Processo de Poisson Homogéneo (HPP) se a distribuição em causa é a exponencial negativa, caracterizada por uma função de risco constante. Desta forma a sequência cronológica dos tempos até à avaria deixa de ter importância para a análise. Esta é uma característica que se verifica durante o período de vida útil dos bens reparáveis. Se N(t) for o número de avarias ocorridas até ao instante "t", a taxa de avarias ou taxa de ocorrência de falhas de um sistema (ROCOF) é definida como sendo a derivada em ordem ao tempo do número esperado de falhas até ao instante "t".

De acordo com a representação da curva da banheira da Figura 2.4, referente ao comportamento típico da taxa de avarias para bens reparáveis, a duração do período de vida útil pode ser influenciada por factores como o tipo de controlo de qualidade e política de manutenção aplicados, assim como pelo nível de solicitações exigido. Assim, estes factores irão condicionar o comportamento da taxa de avarias, conforme ilustrado na Figura 2.7.

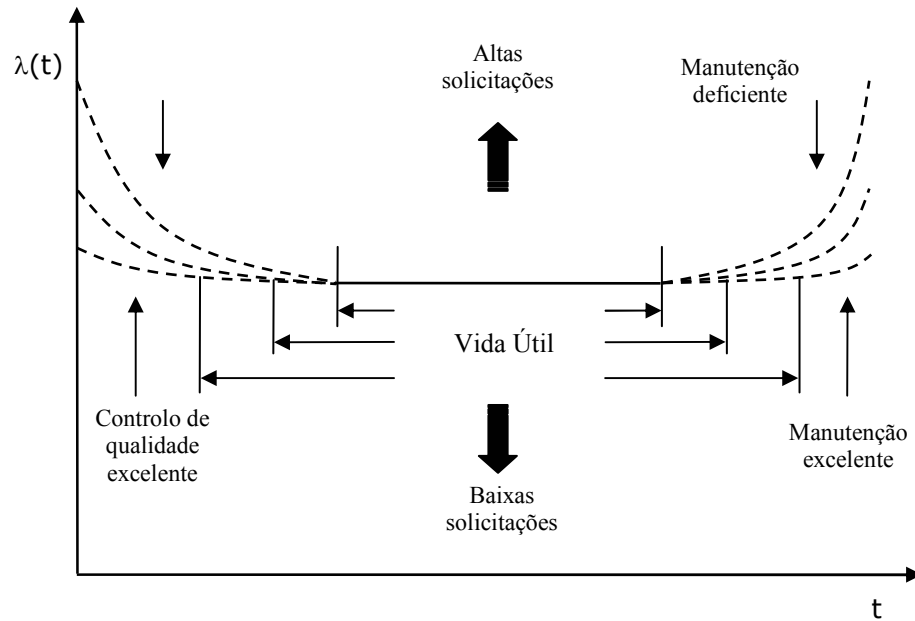



Figura 2.7 – Influência de alguns factores na taxa de avarias

2.3.7.3 – Tempo médio de vida

Outro conceito de referência quando se menciona a probabilidade de sobrevivência é o que diz respeito à vida média expectável de um bem.

Tendo um historial sobre tempos entre as sucessivas avarias de um determinado bem, o tempo médio até à avaria pode ser definido como a média aritmética da variável aleatória "idade até à avaria".

Para distribuições contínuas, o tempo médio para a avaria (MTTF - *Mean Time To Failure*), quando nos referimos a bens não reparáveis, ou tempo médio entre avarias (MTBF - *Mean Time Between Failures*), quando se trata de bens reparáveis, é dada por:

$$\text{MTTF} = \int_0^\infty t.f(t).dt = \int_0^\infty R(t).dt \qquad (2.10)$$

Este tipo de grandeza é muito popular, uma vez que de uma forma simples dá uma ideia da fiabilidade de qualquer bem. Por vezes também é referido o MTTFF (*Mean Time To First Failure*), usado fundamentalmente nas análises dos tempos até a ocorrência da

primeira e única avaria, como é o exemplo de equipamentos do tipo satélites, mísseis, munições, etc...

De acordo com o exposto nos parágrafos anteriores, a Figura 2.8 mostra numa única representação as várias curvas representativas da vida de um bem (Assis, 2010).

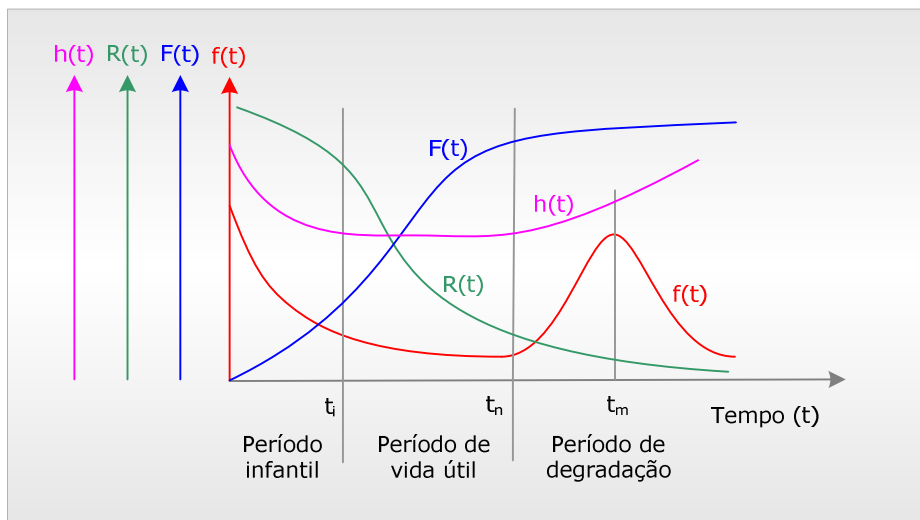



Figura 2.8 – Representação gráfica das várias funções de fiabilidade
[Fonte: Assis (2010)]

Estas funções, ao representar a vida de um bem, também são vulgarmente designadas por "leis de vida". No entanto, há que ter em atenção alguns pormenores, nomeadamente referir que as referidas curvas correspondem a bens reparáveis (sistemas) e que a aplicabilidade do termo "lei de vida" deve ser ponderada para cada caso particular.

2.3.7.4 – Fiabilidade condicional

Não se pode deixar de referir um outro conceito, que tem a ver com o cálculo do valor da fiabilidade para uma nova missão de duração "Δt" após o bem em causa ter acumulado uma duração de vida "t". Trata-se da chamada fiabilidade condicional (ou fiabilidade de missão), que pode ser expressa da seguinte forma:

$$R(\Delta t \mid t) = \Pr(t_f > t_1 = t + \Delta t \mid t_f > t) \qquad (2.11)$$

ou

$$R(\Delta t \mid t) = \frac{R(t+\Delta t)}{R(t)} \qquad (2.12)$$

Estas expressões significam exactamente a probabilidade do bem só avariar com uma idade superior à missão considerada (Δt) e com a garantia ou condição que o mesmo se encontra a funcionar em "t", relativo ao limite inferior do intervalo correspondente à missão em estudo.

Estes temas, assim como uma apresentação dos tipos de distribuições mais comuns em análises de fiabilidade, serão desenvolvidos com mais detalhe em futuros parágrafos. Pretende-se neste momento enquadrar o tema e mostrar de uma forma global como se pode determinar a fiabilidade, assim como outras métricas com ela relacionadas.

2.3.8 – Fiabilidade de Componentes

Quando não se possui uma base de dados credível acerca da fiabilidade de um componente, ou outra informação que nos permita calcular com relativa facilidade essa mesma fiabilidade, teremos que recorrer à análise de dados de vida, sejam eles retirados do contexto operacional (em fase de exploração) ou provenientes de ensaios (normais, acelerados ou altamente acelerados).

Tal como referido anteriormente, quando se analisam as avarias de determinados componentes, o conhecimento da função densidade de probabilidade de falha desses componentes torna-se uma ferramenta fundamental para visualizar como ocorrem as avarias durante a sua vida e como as mesmas se encontram estatisticamente distribuídas.

Conforme indicado em 2.3.7.1, após o conhecimento da função densidade de probabilidade de falha, podemos determinar outras funções, como a fiabilidade, a probabilidade de falha ou a função de risco. Porém, esta tarefa de análise de dados de vida pode não ser tão simples como isso e, quando mal conduzida, pode levar a resultados errados.

A primeira etapa da análise de dados de vida de um bem consiste em escolher a forma como esses dados serão estudados, nomeadamente se os mesmos são analisados individualmente ou em grupo.

A etapa seguinte refere-se à definição do tipo de dados que possuímos, nomeadamente se são todos tempos até à avaria ou se existem dados suspensos (ou censurados) referentes a tempos de bom funcionamento desde as últimas avarias até ao momento da análise, ou ainda se os dados se referem a intervalos de tempo (se por exemplo apenas sabemos que a avaria ocorreu durante um turno de trabalho).

Segue-se a selecção da distribuição estatística. Nas análises clássicas de fiabilidade, a determinação do tipo de distribuição que mais se ajusta a um determinado número de dados existentes pode ser efectuada com recurso a vários testes ou métodos (Qui-quadrado, Kolmogorov-Smirnov, etc.).

Após se ter adoptado a distribuição que mais se ajusta aos dados, há que estimar os parâmetros característicos dessa distribuição. Para esse efeito existem basicamente três metodologias:

- Método Gráfico;
- Método dos Mínimos Quadrados (Análise de Regressão);
- Método da Máxima Verosimilhança (MLE).

O Método Gráfico (*probability plotting*) implica o uso de papéis especialmente concebidos para o efeito, linearizando a função de probabilidade de falha acumulada. Nestes papéis, ao eixo das abcissas correspondem os tempos até à avaria (TTF), enquanto no eixo das ordenadas se indicam as probabilidades de avaria "F(t)" (em percentagem). Estas probabilidades poderão ser determinadas através da categoria mediana[5] de cada avaria ou através do método não paramétrico Kaplan-Meier.

O método dos Mínimos Quadrados (*Least Squares Parameter Estimation*), ou Regressão Linear, é a versão matemática do método gráfico anteriormente referido, ajustando uma recta a um conjunto de pontos, onde a soma dos quadrados da distância dos pontos à

---

[5] A Categoria Mediana (*Median Rank*) pode ser obtida para qualquer ponto aplicando a equação da distribuição binomial comulativa para uma dimensão da amostra "N" e para uma ordem de "j" da avaria, igualando a referida equação a 0,50. Em alternativa, a Categoria Mediana poderá ser determinada através da Aproximação de Bernard.

recta ajustada é mínimo, quer na vertical (regressão em "y"), quer na horizontal (regressão em "x"). O coeficiente de correlação (ρ) significa o quanto os pontos estão alinhados com a linha de regressão linear. Quanto mais alinhados, melhor a correlação para a distribuição adoptada, correspondendo a valores de correlação próximos de ± 1. Este método é indicado quando se trata de dados completos (não censurados).

Do ponto de vista estatístico o método da Máxima Verosimilhança (MLE) é, regra geral, considerado o método mais robusto para estimar os parâmetros de uma distribuição. A ideia básica por trás do método MLE é obter os valores mais verosimilhantes para os parâmetros, que melhor descrevem a distribuição em causa. Como características relativas à aplicação deste método pode-se indicar como vantagem a sua consistência e eficiência assimptótica, ou seja, à medida que aumenta a dimensão da amostra (dados) mais os resultados convergem para os valores correctos e maior a precisão da estimativa. Desta forma, é aconselhável que a dimensão da amostra seja de certa forma grande, apontando-se como ideal um valor acima de trinta registos de avarias. Assim, para poucos dados, ou em situações onde existam tempos censurados, a descrepancia dos resultados obtidos é maior. Para a aplicação deste método, devido à sua complexidade, é necessário recorrer a programas informáticos.

Desta forma, recomenda-se a utilização do Método dos Mínimos Quadrados (Técnica de Regressão) para pequenas amostras, sem dados censurados, e a utilização do método da Máxima Verosimilhança para grandes amostras, mesmo que contendo dados censurados.

Quando se trata de variáveis contínuas, as principais distribuições estatísticas utilizadas em estudos de fiabilidade de componentes são:

- Distribuição Weibull (1, 2 ou 3 parâmetros);
- Distribuição Exponencial (1 ou 2 parâmetros);
- Distribuição Normal (2 parâmetros);
- Distribuição Lognormal (2 parâmetros);

As definições e respectivas equações relativas às distribuições estatísticas anteriormente referidas podem ser encontradas na vasta literatura existente nesta área.

No **Anexo I** apresentam-se algumas considerações relativas às funções de densidade de probabilidade de falha e de fiabilidade das distribuições mais utilizadas.

2.3.9 – Fiabilidade de Sistemas

Pode-se definir um sistema como um conjunto de componentes, combinados entre si de modo específico, correspondendo a arranjos físicos (série, paralelo, compostos, complexos), para atingir as funções operacionais desejadas, desempenho, fiabilidade e custos que satisfaçam as necessidades do utilizador final. No fundo, o termo sistema pode significar um equipamento ou um conjunto de componentes que prestam um determinado serviço ou cumprem uma determinada função.

Os diferentes tipos de componentes, a sua quantidade, qualidade e arranjos, quando combinados entre si, apresentam um efeito directo na fiabilidade do referido sistema. No cálculo da fiabilidade de sistemas também se deve ter em conta que os componentes em paralelo correspondem a redundâncias activas ou passivas (*standby*) e que todas as avarias de causa comum (CCF = *Common Cause Failures*) devem ser consideradas.

Cada componente do sistema terá um índice de importância com base no que se considera a sua influência individual no valor da fiabilidade do sistema, sendo para tal fundamental conhecer a sua distribuição de avarias e a sua correspondente posição no sistema em análise.

De um modo geral a aplicação de redundâncias baseia-se no pressuposto de que o componente primário não permite alcançar o desejado valor de fiabilidade, ou o custo para o fazer atingir é elevado. A utilização de redundâncias é, por exemplo, justificada em sistemas críticos, onde a consequência da avaria poderá levar a situações catastróficas. As redundâncias podem ser activas ou passivas, necessitando estas últimas de detectores-comutadores (ou sensores-comutadores), devendo também ser considerada a sua probabilidade de falha nos sistemas onde estejam incluídos.

Convém referenciar que por vezes existe uma diferença entre o modelo físico e o modelo de fiabilidade. Isto quer dizer, por exemplo, que podemos ter fisicamente um arranjo tipo série, como por exemplo duas caldeiras ligadas em série para aquecer água a uma determinada temperatura, mas em termos de fiabilidade as duas caldeiras funcionam uma como reserva da outra, uma vez que a temperatura pretendida é alcançada por qualquer um dos dois equipamentos, logo fiabilisticamente o sistema é calculado como um sistema paralelo activo.

2.3.10 – Metodologias e ferramentas de apoio à análise fiabilistica

As metodologias para estimar a fiabilidade de sistemas necessitam na maior parte dos casos de conhecimentos básicos da teoria geral das probabilidades, assim como a definição de alguns dos seus conceitos fundamentais (espaço amostral, reunião, intersecção, etc.). No **Anexo III** encontram-se descritos alguns conceitos básicos, teoremas e axiomas referentes a esta teoria.

O cálculo ou determinação da fiabilidade de um sistema deve considerar a previsão analítica de vida, ou seja, como a duração influencia a fiabilidade. Quando este método não for possível, dever-se-á utilizar um método de simulação.

Para a determinação da probabilidade de falha (ou sucesso) de um sistema é possível recorrer a várias metodologias, como RBD (*Reliability Block Diagrams*), FTA (*Fault Tree Analysis*), ETA (Event Tree Analysis), PN (*Petri Nets*), modelos de Markov ou modelo híbridos, muitas vezes com recurso a simulação. Cada uma destas técnicas tem as suas vantagens e desvantagens e a sua escolha depende do sistema a ser modelado. Neste capítulo pretende-se referir algumas das metodologias de uma forma simples, apresentando as suas características principais.

2.3.10.1 – RBD (*Reliability Block Diagram*)

Os diagramas de blocos de fiabilidade (RBD) são gráficos directos que representam os elementos que constituem um sistema e a disposição lógica como os mesmos se encontram relativamente uns aos outros.

O sistema é construído com recurso a blocos que representam cada elemento, ligados entre si por linhas ou conectores. A análise é efectuada numa lógica de sucesso, ou seja, a questão é colocada em função do sucesso do sistema.

O fluxo lógico de um diagrama de blocos parte de um nó inicial, colocado à esquerda do diagrama, e termina num nó final ou de saída, colocado à sua direita. Os blocos são colocados construtivamente entre os dois nós acima referidos, de acordo com os vários tipos de arranjos lógicos.

Os diagramas de blocos servem para modelar sistemas complexos. Para cada bloco são fornecidos dados, permitindo efectuar cálculos para determinar taxas de avarias, MTBF, fiabilidade e disponibilidade dos sistemas analisados. Alterando a configuração dos blocos, os resultados também serão diferentes. Assim, poderão ser comparadas várias configurações na tentativa de encontrar a melhor estrutura global de um sistema.

Como qualquer outra metodologia, o diagrama de blocos de fiabilidade tem vantagens e desvantagens quando comparado com outros métodos de representação. Essas desvantagens prendem-se fundamentalmente com os componentes básicos e o tipo de construção usada no diagrama, não permitindo traduzir determinadas interacções entre os componentes e afastando-se por vezes do objectivo principal, que é o representar fielmente as relações lógicas através de um sistema de blocos, em termos fiabilísticos.

Normalmente os sistemas representados por blocos de fiabilidade apresentam configurações tipo série, paralelo ou combinações destes dois, ou ainda arranjos específicos resultando nos sistemas designados por complexos. No entanto, quando se trata de representar dependências funcionais, componentes em “*standby*” ou sequências de falhas, a dificuldade aumenta, sendo muitas vezes impossível concretizar esse tipo de representação.

O **Anexo IV** ao presente documento descreve a forma como determinar analitica e empiricamente a fiabilidade de um sistema através de blocos funcionais, partindo dos dados fiabilisticos individuais dos elementos que o constituem e da forma como os mesmos se encontram organizados.

2.3.10.2 – ETA (*Event Tree Analysis*)

A metodologia de Análise de Árvore de Acontecimentos (ETA = *Event Tree Analysis*) é uma ferramenta que segue a lógica indutiva, através de uma sequência de acontecimentos a partir de um incidente ou acontecimento inicial, e onde são equacionados os vários cenários subsequentes possíveis de ocorrer.

As consequências de um acontecimento acidental são determinadas pela forma como a sua progressão é afectada pelas falhas posteriores na operação das funções de segurança[6], por erros humanos e por outros factores como as condições ambientais.

A Análise de Árvore de Acontecimentos é um diagrama lógico que cobre o referido acontecimento inicial ou iniciador e toda a sequência de propagação até aos vários cenários ou consequências finais, assumindo as falhas e sucessos das funções de segurança que são disponibilizadas à medida que o acidente se propaga. Cada acontecimento da árvore será condicional à ocorrência dos acontecimentos anteriores da cadeia.

Os resultados de cada acontecimento são normalmente assumidos na sua forma binária (verdadeiro ou falso, sim ou não), podendo no entanto incluir multiplas saídas (ex. sim, parcialmente, não).

A Análise de Árvore de Acontecimentos insere-se na maior parte das análises de risco, podendo ser usada como uma ferramenta de projecto para demonstrar, por exemplo, a eficácia de um sistema de protecção. A sua informação pode ser qualitativa, quantitativa ou ambas, dependendo dos objectivos da análise. Numa análise de risco quantitativa (QRA – *Quantitative Risk Assessment*) as Árvores de Acontecimentos podem ser efectuadas de forma independente ou ser elaboradas no prolongamento de uma Análise de Árvore de Falhas (Rausand & Hoyland, 2004).

Uma Análise de Árvore de Acontecimentos qualitativa é normalmente efectuada em seis etapas, nomeadamente:

1. Identificação de um acontecimento inicial (acidental) que possa levar a consequências indesejadas;
2. Identificação das funções de segurança que estão presentes para fazer face ao acontecimento inicial;
3. Construção da Árvore de Acontecimentos;
4. Descrição das sequências de acontecimentos resultantes;
5. Cálculo da probabilidade ou frequências das consequências identificadas;
6. Compilação e apresentação dos resultados da análise.

[6] Ver Capítulo III para mais informações sobre esta temática

A identificação do acontecimento inicial é bastante importante, podendo ser realizada através de outra técnica como uma Análise de Modos de Falha, Efeitos e Criticidade (FMECA), Análise Preliminar de Perigos (PHA – *Preliminary Hazard Analysis*) ou uma Análise de Perigos e Operabilidade (HAZOP – *Hazard and Operability Analysis*).

Relativamente aos vários cenários possíveis, deve haver uma forma clara de os apresentar, fruto de uma hierarquização efectuada de acordo com a sua criticidade. Desta forma, a estrutura do diagrama mostra todas as sequências e progressão do acidente até aos vários cenários alcançados, permitindo especificar onde se deverão incluir medidas (procedimentos) adicionais ou sistemas de segurança. Também se podem dividir os vários cenários resultantes em categorias, como por exemplo no que respeita à perda de vidas, danos patrimoniais ou danos ambientais.

2.3.10.3 – PN (*Petri Nets*)

As Redes de Petri foram desenvolvidas e apresentadas por Carl A. Petri em 1962, e são usadas fundamentalmente como uma representação gráfica de processos dinâmicos, especialmente aqueles que possuem ligações internas complexas (Schneeweiss, 2004). Nestas representações gráficas usam-se nós (*nodes*) ou vértices (*vertices*) unidos por ligadores (*edges*) indicando um determinado sentido. Devido a esta última característica, as Redes de Petri também se designam por gráficos directos (*digraphs*).

Apesar das Redes de Petri já terem alguns anos, a sua utilização não tem tido grande divulgação no campo da fiabilidade, embora se constate uma grande potencialidade da sua aplicação. No entanto, observa-se uma inversão desta tendência através de alguns estudos recentes recorrendo à utilização desta técnica para modelação de sistemas com vista à determinação da sua fiabilidade, como é o exemplo de um estudo que se encontra a ser realizado para a Força Aérea Inglesa (*Royal Air Force*) (Shew *et al*, 2010), onde se pretende modelar a fiabilidade de aviões militares para missões tendo em conta os períodos livres de manutenção, recorrendo às Redes de Petri.

Os nós podem ser de dois tipos, nomeadamente os designados por “locais” (*places*), representados por circulos, e as “transições” (*transitions*) representadas por quadrados. Os “locais” contêm pontos indicados a preto chamados “marcas” (*tokens*). São estas marcas que se movem de local para local após o atraso indicado nas transições,

conferindo desta forma uma dinâmica ao sistema. A Figura 2.9 mostra a situação antes e depois do movimento referente a uma transição de duração "D".

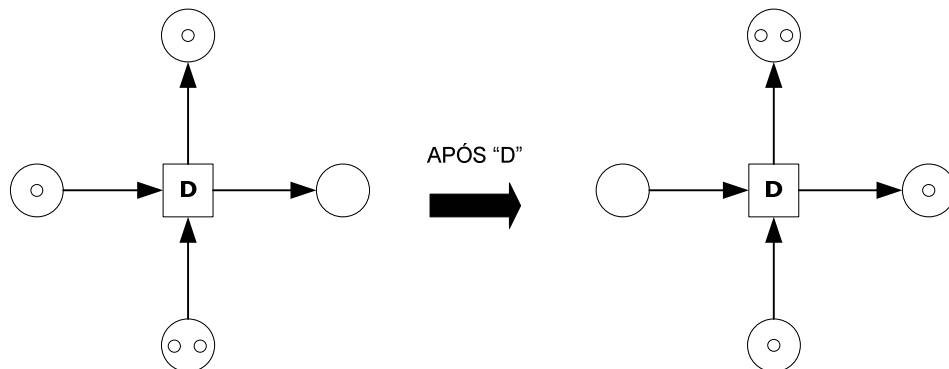



Figura 2.9 – Exemplo de uma Rede de Petri

Dado que no presente documento a metodologia utilizada para a análise fiabilistica não se centrou nesta técnica (Redes de Petri), pretendeu-se apenas fazer a referência à mesma, abrindo campo a futuros e promissores desenvolvimentos.

2.3.10.4 – FTA (*Fault Tree Analysis*)

A avaliação probabilística de segurança (PSA – *Probabilistic Safety Assessment*) é uma metodologia sistemática realizada e aplicada para estimar a fiabilidade e segurança de sistemas complexos (Volkanovski, 2009). Dois métodos básicos usados na PSA são as Árvores de Acontecimentos (já referidas) e as Árvores de Falhas.

A Árvore de Falhas é uma ferramenta usada para identificar e avaliar as combinações de acontecimentos indesejáveis no contexto da operação de um sistema que podem levar a um estado indesejável do mesmo, representado pelo acontecimento de topo. Os acontecimentos básicos são as partes finais da Árvore de Falhas que representam estados de falha de componentes (ou sistemas) ou falhas de cumprimento de uma determinada função. A Árvore de Falhas clássica é representada por um conjunto de equações baseadas na álgebra de Boole.

A Árvore de Falhas é um fluxograma lógico construído a partir de uma análise dedutiva, onde em cada acontecimento mais geral se deduzem os acontecimentos particulares que, na ordem natural dos acontecimentos, o podem originar.

O conceito de Árvore de Falhas foi inicialmente desenvolvido por H. Watson em 1961, na *Bell Telephone Laboratories*, e tem sido modificado muitas vezes desde então (Schneeweiss, 1999). Segundo Sinnamom & Andrews (1997) esta técnica teve a sua primeira utilização durante um estudo ao sistema de controlo do lançamento dos mísseis balísticos intercontinentais Minuteman.

Muitas indústrias utilizam o método da Análise de Árvore de Falhas no estudo da adequabilidade de um sistema numa perspectiva de risco e fiabilidade. Este método fornece uma representação da lógica de um modo de falha do sistema, que pode ser analisada para prever o desempenho do mesmo (Sun & Andrews, 2004).

A Árvore de Falhas é uma técnica gráfica destinada a entender como pode ocorrer um determinado acontecimento, denominado como falha principal ou evento de topo de um sistema, através da análise e identificação dos possíveis estados de falha, designados por acontecimentos primários dos subsistemas ou componentes, considerados individualmente e tendo em conta os arranjos funcionais entre os mesmos. Esta metodologia visa fundamentalmente satisfazer requisitos de segurança e melhorias de projecto ou processo, determinando a probabilidade de ocorrência do acontecimento de topo.

Como referido, é um método que se aplica com grande frequência em sistemas de segurança, como os existentes em instalações nucleares ou plataformas de petróleo *offshore*. A importância da Análise de Árvore de Falhas em sistemas de segurança reside no facto de se poder obter uma descrição completa das várias causas da falha do sistema, sendo assim possível identificar e rectificar qualquer problema de projecto (Sinnamom & Andrews, 1997).

A Figura 2.10 mostra um exemplo de uma Árvore, com os vários tipos de avarias que podem ocorrer nos componentes, subsistemas e/ou sistemas, ligadas por portas lógicas tipo "E" (*AND*) e "OU" (*OR*). Com este exemplo simples pretende-se mostrar e perceber como pode ocorrer a falta de energia (evento de topo) numa instalação que possua uma ligação à rede eléctrica (pública) e um gerador de emergência como alternativa a essa rede.

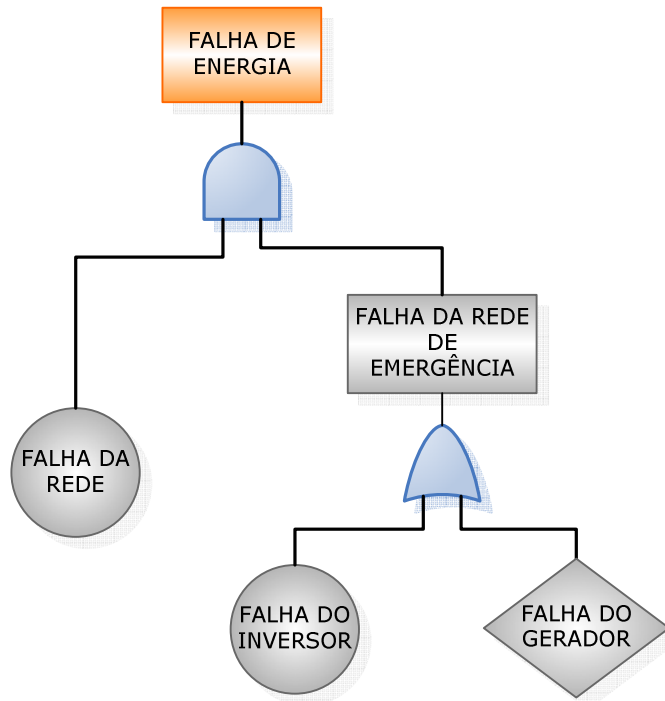



Figura 2.10 – Exemplo de uma Árvore de Falhas

A fiabilidade de um sistema é afectada não só pelas fiabilidades dos componentes, mas também pela forma como os mesmos se encontram relativamente entre si e pelas protecções existentes. A Análise de Árvore de Falhas (FTA) é do tipo de cima para baixo (*top down*), ao contrário, por exemplo, da Análise de Modos e Efeitos de Falha (FMEA – *Failure Modes and Effect Analysis*).

Como referido anteriormente, começa-se pelo acontecimento indesejado, sendo a estrutura de toda a árvore estabelecida normalmente através da utilização de portas lógicas tipo “E” (*AND*) e “OU” (*OR*) para combinar os acontecimentos básicos ou intermédios. Trata-se de um método bastante testado, havendo software especializado para a sua análise. A probabilidade do acontecimento inicial (evento de topo) se verificar pode ser calculada através das probabilidades dos denominados eventos básicos. As Árvores de Falhas também são uma ferramenta importante na ajuda do diagnóstico após a ocorrência de avarias ou acidentes graves.

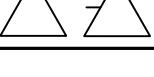
Constata-se que uma Árvore de Falhas é um “negativo” do diagrama (lógico) do sistema formado pelas funções correspondentes aos acontecimentos de sucesso considerados, ou seja, as referidas no Diagrama de Blocos de Fiabilidade anteriormente referido. O

Diagrama de Blocos é analisado numa lógica de sucesso do sistema, enquanto a Árvore de Falhas é vista numa óptica de insucesso ou falha.

Na correspondência das Árvores de Falhas com a álgebra Booleana pode-se dizer que as portas lógicas "OU", "E" e "NÃO" combinam acontecimentos da mesma forma que as operações Booleanas "união", "intersecção" e "complementar", respectivamente.

Os principais objectivos de uma análise utilizando FTA passam por:

- Aumentar a segurança funcional, operacional e ambiental;
- Avaliar e aumentar a fiabilidade dos sistemas;
- Identificar os componentes mais frágeis do ponto de vista da fiabilidade do sistema;
- Compreender melhor o sistema;
- Identificar os efeitos das avarias de causa comum (CCF – Common Cause Failures);
- Avaliar o risco de um determinado produto;
- Fornecer documentação com resultados analíticos;
- Investigar acidentes ou incidentes;
- Analisar a influência de redundâncias;
- Analisar e reduzir os erros humanos na operação, numa lógica funcional.

Com a aplicação da metodologia FTA pretende-se fundamentalmente ter uma visão clara e detalhada do projecto, processo ou sistema, e uma diminuição das falhas críticas e acidentes considerados graves. A grande vantagem de uma FTA prende-se com o facto de ser um método orientado para os acontecimentos e ser um método gráfico, o que a torna de certa forma de fácil compreensão. A grande desvantagem de uma FTA relaciona-se com a circunstância dos acontecimentos indesejáveis que conduzem até ao acontecimento de topo terem de ser conhecidos por antecipação, necessitando também que o analista tenha conhecimento profundo sobre o sistema, podendo dessa forma por vezes ser um processo moroso.

As seguintes etapas devem ser seguidas na estruturação e aplicação de uma Análise de Árvore de Falhas:

1. Definir com clareza o acontecimento de topo (ex. falha de um produto);
2. Estruturar o sistema para se ter uma visão clara e objectiva (identificar componentes, pontos críticos e níveis de risco);

3. Identificar as possíveis falhas, com os seus modos, efeitos e causas, bem como os controlos existentes;
4. Construir a Árvore com o maior detalhe possível, mas com objectividade (utilizar a simbologia e portas lógicas normalizadas, falhas dependentes e independentes, arranjos físicos, redundâncias);
5. Calcular as probabilidades em função dos dados disponíveis (teste ou utilização) e durações, através de métodos analíticos (meios informáticos);
6. Avaliar os resultados obtidos para a falha principal (ou acontecimento de topo) ou falhas primárias, se necessário;
7. Implementar acções correctivas, fundamentalmente para os bens críticos (com baixa fiabilidade).

A Tabela 2.1 apresenta a simbologia normalmente utilizada na construção gráfica de uma Árvore de Falhas, referentes a portas lógicas e acontecimentos.

Tabela 2.1 – *Simbologia lógica e nomenclatura mais usada em Análises de Árvore de Falhas*

	Porta lógica “E” (Gate “AND”) – O output só se verifica se um e outro input se verificarem
	Porta lógica “OU” (Gate “OR”) – O output verifica-se se um ou outro dos inputs se verificarem - também designado por “OU Inclusivo”
k/n	Porta lógica “k de n” (“Voting Gate”) – O output verifica-se se pelo menos “k” dos “n” inputs se verificarem
	Acontecimento “FALHA BÁSICA” ou “FALHA PRIMÁRIA”
	Acontecimento “NÃO DESENVOLVIDO” - Considera-se não ser necessário desenvolver mais o acontecimento em termos de causas
	Acontecimento “FALHA DE TOPO” ou DESCRIÇÃO INTERMÉDIA
	Acontecimento “CASA” - Pode ocorrer ou não ocorrer com certeza (TRUE or FALSE)
	Porta lógica “INIBIÇÃO” (“INHIBIT Gate“) – O input produz o output quando o acontecimento condicional existir
	Acontecimento “CONDICIONAL” usado com a porta Inibição
	Transferência, Repetição ou Sub-Árvore correspondente ao respectivo ramo, assinalado no fluxograma lógico

A análise de uma Árvore de Falhas faz-se normalmente em duas fases: uma análise **qualitativa** seguida de uma análise **quantitativa**. A análise qualitativa traduz-se por obter as várias combinações de acontecimentos que podem causar a falha ou evento de topo (MCS - *minimal cut sets*), enquanto a análise quantitativa se baseia no cálculo da probabilidade ou frequência com que a falha (estado) do sistema pode ocorrer. A análise qualitativa pode ser efectuada recorrendo a Diagramas de Decisão Binários (BDD – *Binary Decision Diagrams*) (Sinnamom & Andrews, 1997) ou outros algorítmos computacionais.

Um conjunto de corte (*cut set*) de uma Árvore de Falhas é uma lista de acontecimentos básicos ou falhas de componentes, que quando ocorrem, o acontecimento de topo também ocorre, ou seja, o sistema encontra-se em falha. Todos os conjuntos de corte (*cut sets*) correspondem a todos os modos como o sistema pode falhar. Um conjunto de cortes mínimo (*minimal cut set*) refere-se à mais pequena combinação de componentes que levam à falha do sistema (ou ocorrência do acontecimento de topo). Se algum dos acontecimentos básicos de um conjunto de cortes mínimo é removido do conjunto, a falha já não ocorrerá. A listagem completa do conjunto dos cortes mínimos é a maior preocupação da análise qualitativa de uma Árvore de Falhas (Sinnamom & Andrews, 1997). Os conjuntos de corte mínimos compostos por um elemento designam-se por conjuntos de corte mínimos de primeira ordem, com dois elementos designam-se por segunda ordem e assim sucessivamente. Os conjuntos de ordens mais baixas são aqueles que devem ser analisados, de forma a serem eliminados e assim melhorar o desempenho do sistema.

Após a determinação do conjunto dos cortes mínimo (MCS), a forma mais correcta de determinar a probabilidade do acontecimento de topo será utilizar o método da inclusão-exclusão (Andrews & Moss, 2002) (Cepin & Mavko, 2002). Desta forma, se a Árvore de Falhas tem “n” conjuntos de corte mínimos K_i, onde i=1, 2, ..., n, então o acontecimento de topo existe se pelo menos um conjunto de corte mínimo existir, ou seja:

$$T = K_1 + K_2 + ... + K_n \tag{2.13}$$

$$P(T) = \left(\bigcup_{i=1}^{n} K_i \right) \tag{2.14}$$

então, usando a expressão da expansão inclusão-exclusão, fica:

$$P(T)=\sum_{i=1}^{n}P(K_i)-\sum_{i=2}^{n}\ \sum_{j=1}^{i-1}P(K_i\cap K_j)+...+(-1)^{n-1}.P(k_1\cap k_2\cap...\cap k_n)$$

(2.15)

Como este cálculo poderá ser na maioria dos casos fastidioso e manualmente impraticável, uma vez que numa Árvore de Falhas podem-se obter milhares de conjuntos de corte mínimos, então fazem-se aproximações, verificando-se que o primeiro termo da expressão é mais significativo que o segundo, o segundo que o terceiro e assim sucessivamente. A série converge com cada termo a dar cada vez um menor contributo para o valor da probabilidade final. Se bloquearmos a série num número impar ficaremos com o limite superior, e se for com um número par, com o limite inferior. Desta forma, o valor exacto da probabilidade encontra-se entre estes dois valores limite.

$$\sum_{i=1}^{n}P(K_i)-\sum_{i=2}^{n}\ \sum_{j=1}^{i-1}P(K_i\cap K_j)\leq P(T)\leq\sum_{i=1}^{n}P(K_i) \qquad (2.16)$$

O valor limite superior para a probabilidade do acontecimento de topo é conhecido como a "*aproximação ao evento raro*", uma vez que se torna um valor certo se as avarias dos componentes são raras. Andrews e Moss (2002) apresentam ainda outra forma mais apurada para o cálculo do limite superior, designada por "*minimal cut set upper bound*".

Volkanovski et al. (2009) calculam a probabilidade de ocorrência do acontecimento de topo (*P*) através da seguinte expressão:

$$P=\sum_{i=1}^{n}P_{MCS_i} \qquad (2.17)$$

onde a probabilidade de cada conjunto de corte mínimo (P_{MCS}) é determinada usando a relação de ocorrência simultânea de acontecimentos independentes:

$$P_{MCSi}=\prod_{j=1}^{m}P_j \qquad (2.18)$$

ou seja, o produto das probabilidades dos acontecimentos básicos (P_j) que fazem parte desse conjunto.

Como a obtenção da listagem dos conjuntos de corte mínimos pode representar um trabalho árduo quando uma Árvore de Falhas não contem acontecimentos mutuamente exclusivos ou esta for muito extensa, são normalmente utilizados métodos de geração de cortes mínimos. Destes métodos destaca-se um algoritmo designado por MOCUS (*Method of Obtaining Cut Sets*), desenvolvido por Fussell e Vesely em 1972.

Este algoritmo é efectuado de cima para baixo (*top-down*) e assenta no facto das portas lógicas "OU" terem o efeito de aumentar o número de conjuntos de corte e as portas "E" aumentarem o tamanho ou a ordem desses conjuntos (Andrews & Moss, 2002).

Podem ainda ser referidos outros métodos como o Esary Proschan (assumindo que todos os conjuntos de corte são independentes, incluindo algumas simplificações) ou métodos mais exactos com algoritmos de geração de conjuntos de corte, como o MICSUP (*Minimal Cut Set Upwards*), similar ao MOCUS mas com uma abordagem de baixo para cima (*bottom-up*), ou o ZBDD (*Zero-Suppressed Binary Decision Diagrams*), baseado em Diagramas de Decisão Binária (BDD).

A análise quantitativa de uma Árvore de Falhas identifica a probabilidade de ocorrência do acontecimento de topo e de cada conjunto de corte mínimo identificado na fase qualitativa. Esta quantificação necessita de dados de entrada para cada acontecimento situado no nível mais baixo, como as probabilidades de falha, as taxas de avaria, as taxas de reparação ou a frequência das avarias, conforme os objectivos em jogo. Assim, poderá ser calculada a indisponibilidade ou probabilidade de falha do sistema.

Outro tipo de informação que se pode extrair de uma Árvore de Falhas é um conjunto de medidas indicando a contribuição de cada componente para a falha do sistema, também designadas por medidas de importância[7].

Na quantificação de uma Árvore de Falhas há que ter em conta se os acontecimentos são independentes, ou seja, se não se repetem na estrutura ou se não há interesse em ter em conta a ordem temporal da sequência dos mesmos. Neste caso, a probabilidade do acontecimento de topo pode ser obtida através das probabilidades dos acontecimentos

[7] Ver Capítulo V

básicos, começando pela base da Árvore. Trata-se de uma abordagem simples, mas infelizmente não aplicável à maioria das Árvores de Falhas, uma vez que em muitos casos os acontecimentos básicos se repetem e normalmente a ordem em que os mesmos ocorrem é importante. Ignorar este aparente pormenor pode levar ao cálculo de probabilidades para o acontecimento de topo sobre-estimadas ou sub-estimadas, dependendo da estrutura da Árvore em análise (Andrews & Moss, 2002).

2.3.11 – Necessidade de evoluir das Árvores de Falhas Estáticas para as Árvores de Falhas Dinâmicas

A Árvore de Falhas é indubitavelmente uma das ferramentas mais usadas em análises de fiabilidade. Como as Árvores de Falhas tradicionais (ou estáticas) não suportam dependências sequenciais e funcionais entre os componentes, algumas metodologias designadas por dinâmicas foram desenvolvidas para ultrapassar esta situação, destacando-se a utilização das Cadeias de Markov (MC) e as suas extensões, provando ser uma ferramenta versátil para modelar comportamentos dinâmicos complexos de componentes.

No entanto, a utilização das cadeias de Markov apresenta dois grandes problemas: um refere-se à construção manual da cadeia para descrever o comportamento de um sistema, tornando-se em muitos casos uma tarefa complexa, e outro tem a ver com o problema da explosão do número de estados, que aumenta exponencialmente com o número de componentes incluídos no sistema.

Para ultrapassar algumas destas dificuldades, Boudali & Dugan (2005) propõem uma nova metodologia para análise da fiabilidade baseada em redes Bayesianas (BN - *Bayesian networks*) para fazer face ao problema do aumento da complexidade de comportamentos e interacções de componentes, assim como ao crescimento do número de estados.

A questão do crescimento do número de estados de um modelo de Markov também é referida por Guo & Yang (2008), que afirmam que quanto mais complexo for o sistema mais o modelo manual de Markov se torna falível e maior o tempo consumido, o que pode levar os técnicos a evitar a sua utilização (apesar da existência de algumas aplicações informáticas). Estes autores desenvolveram uma metodologia baseada na

decomposição, encontrando subsistemas independentes e tendo em conta zero avarias, avarias seguras, avarias perigosas detectadas e avarias perigosas não detectadas.

Da mesma forma, Knegtering & Brombacher (2000) apresentam um método para reduzir de forma acentuada o esforço de cálculo em análises quantitativas de segurança e fiabilidade para determinação dos SIL (*Safety Integrity Levels*), combinando os benefícios dos modelos de Markov com o modelo RBD (*Reliability Block Diagram*). Através de um exemplo, os autores mostram como um cálculo que demora horas pode ser reduzido a meros segundos com a aplicação de micro modelos de Markov.

Numa FTA, e em alguns casos, a determinação dos conjuntos de corte mínimos (*minimal cut sets*) não depende apenas da ocorrência em simultâneo dos acontecimentos básicos, mas também da sequência com que ocorrem. Long *et al* (2000) chamam SFL (*sequential failure logic*) a este tipo de lógica de avaria. No seu trabalho, estes autores referem uma comparação entre o modelo SFL e o modelo de Markov, onde se mostra que os dois modelos são consistentes entre si.

Resultante do facto das Árvores de Falhas tradicionais (ou estáticas) não poderem conter dependências sequenciais e funcionais entre os componentes de um sistema, foram desenvolvidas algumas ferramentas que convertem a descrição dinâmica de um sistema numa MC, como é o caso do software "*Galileo®*" (2004) desenvolvido na Universidade da Virgínia, nos Estados Unidos da América, fazendo uso de portas lógicas especiais (dinâmicas) e desta forma permitindo modelar substituições de componentes por sobressalentes, falhas que ocorrem apenas quando se verifica uma certa ordem, dependências que propagam a avaria de um componente a outros e avarias que apenas podem ocorrer numa ordem pré-definida.

Desta forma, e resumindo, podem-se considerar as Árvores de Falhas em dois tipos:

- Estáticas;
- Dinâmicas.

Os tipos de portas lógicas utilizadas na construção das Árvores de Falhas definem se estas são estáticas ou dinâmicas. As estáticas contêm apenas portas lógicas estáticas, enquanto as dinâmicas possuem uma ou mais portas lógicas designadas por dinâmicas.

Uma Árvore de Falhas estática pode ser depois classificada como coerente (*coherent*) ou não-coerente (*non-coherent*). Quando se incorpora a lógica negativa (NOT) numa Árvore

de Falhas estática esta torna-se não-coerente. Desta forma, existem acontecimentos positivos e acontecimentos negativos, correspondendo a sucessos e falhas, respectivamente, e que levam à ocorrência do acontecimento de topo. Neste último aspecto incluem-se as portas lógicas NOT, NOR, NAND e XOR. A Tabela 2.2 mostra a simbologia utilizada para as portas lógicas de negação.

Tabela 2.2 – *Portas lógicas de negação usadas em Análises de Árvore de Falhas*

	Porta lógica “NÃO” (Gate “NOT”) – O output só se verifica quando o input não ocorre. Só pode haver um input
	Porta lógica “NÃO OU” (Gate “NOR”). Combinação de uma porta “OR” com uma porta “NOT” - O output verifica-se quando todos os inputs não se verificam
	Porta lógica “NÃO E” (“NAND”) – Combinação de uma porta “AND” com uma porta “NOT” - O output verifica-se quando pelo menos um dos inputs não se verifica
	Porta lógica “OU Exclusivo” (Gate “XOR”) – O output verifica-se se um ou outro dos inputs se verificarem, mas não em simultâneo

Os próximos parágrafos descrevem algumas características relacionadas com a Análise de Árvores de Falhas Dinâmicas (DFTA – *Dynamic Fault Tree Analysis*).

Consideram-se as Árvores de Falhas Dinâmicas (DFT) como uma extensão das Árvores de Falhas (FT), ao definir portas especiais de forma a capturar as dependências e sequências de funcionamento. Trata-se de um modelo híbrido, com uma abordagem modular, servindo para analisar Árvores de Falhas estáticas e dinâmicas, combinando a utilização de Diagramas de Decisão Binária (BDD) para Árvores de Falhas estáticas e Cadeias de Markov (MC) para as dinâmicas.

Se todos os componentes forem considerados não-reparáveis (generalidade) e mutuamente independentes poder-se-á utilizar a metodologia RBD (*Reliability Block Diagram*) ou FTA (*Fault Tree Analysis*) tradicional (por vezes designada de KTT – *Kinetic Tree Theory*). Em sistemas que possuem taxas de avaria e de reparação consideradas constantes tem-se utilizado modelos de Markov, modelos híbridos ou redes de Petri (*Petri Nets*).

Os diagramas de decisão binária (BDD) fornecem um meio rápido para analisar Árvore de Falhas. Com este método a Árvore de Falhas é transformada num BDD, de onde se pode obter directamente o conjunto de cortes mínimos (Sinnamom & Andrews, 1997).

Um BDD é um gráfico acíclico directo onde todos os caminhos do diagrama terminam em um de dois estados, ou o estado "1" que corresponde à falha, ou o estado "0" que corresponde ao sucesso. Todos os caminhos que terminam no estado "1" dão-nos os conjuntos de corte da Árvore de Falhas.

Um BDD é composto por vértices terminais e vértices não-terminais. Os vértices terminais (com valor "0" ou "1") e os não-terminais correspondem aos acontecimentos básicos da Árvore de Falhas. Cada ramal com vértice "0" significa a não ocorrência do acontecimento básico e os ramais com vértice "1" representam a sua ocorrência (falha).

Cada vértice do BDD tem uma estrutura "*if-then-else*" (ite) do tipo:

ite(*X1*,*f1*,*f2*)

que significa que se *X1* falha, então considerar a função *f1*, senão considerar a função *f2*. A função *f1* fica no ramal "1" de *X1* e a função *f2* fica no ramal "0" de *X1*.

A Figura 2.11 mostra um exemplo de uma Árvore de Falhas e o correspondente BDD.

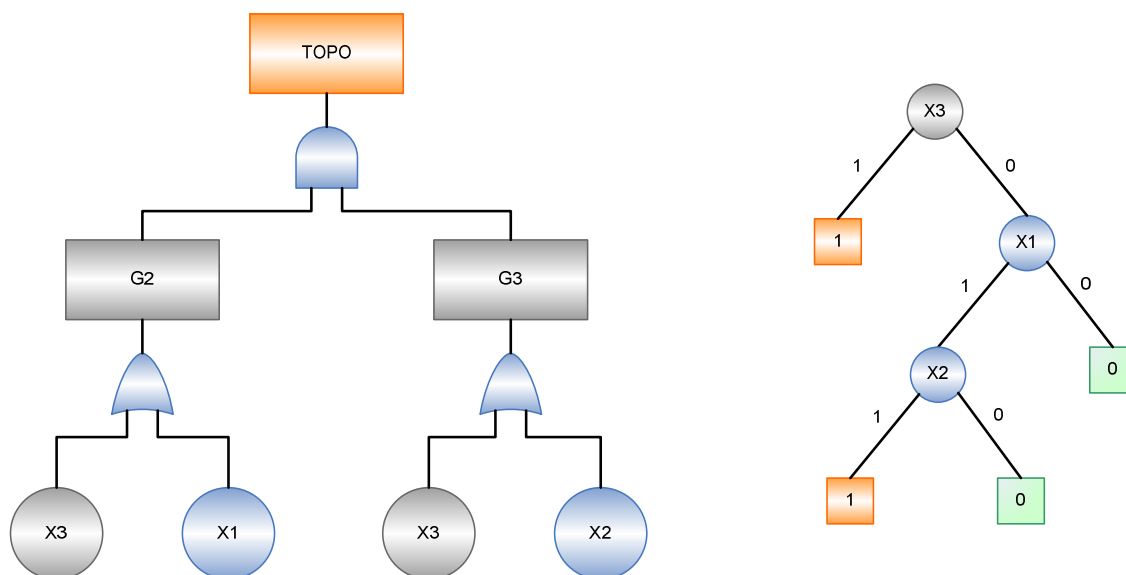



Figura 2.11 – Árvore de Falhas e Diagrama de Decisão Binário

Neste caso simples e específico, aplicando a metodologia referente aos BDD, o corresponde conjunto de cortes mínimos é dado por:

{X3}

{X1, X2}

Nesta temática, relacionada com a utilização de Árvores de Falhas, é de referir também um estudo recente de Shalev & Tiran (2007). Os autores referem que a FTA é uma ferramenta de análise de fiabilidade e segurança, onde normalmente é atribuída uma taxa de avarias constante a cada um dos acontecimentos básicos. No entanto, devido a factores relacionados com a operação e manutenção dos equipamentos, algumas destas taxas de avarias tendem a aumentar, pelo que a fiabilidade calculada inicialmente não corresponde aquela que se regista após um determinado período. Assim, propõem uma nova metodologia baseada na condição (*CBFTA - Condition-Based Fault Tree Analysis)* para ultrapassar esta deficiência das FTA. A informação da FTA vai sendo actualizada com base no controlo de condição que se vai realizando no âmbito de uma manutenção condicional, sendo recalculada periodicamente a probabilidade do evento de topo.

Manian *et al* (1999) referem também que o comportamento à falha de muitos componentes é dependente do tempo, sendo assim descrito mais correctamente através de taxas de avaria variáveis, ao invés do uso de taxas de avarias constantes. Tal como descrito no parágrafo referente à fiabilidade de componentes, esse tipo de comportamento pode ser representado através de outras distribuições, como a de Weibull, a Normal ou a Lognormal. Desta forma, para modelar e avaliar sistemas com valores para as transições que sejam variáveis no tempo, dever-se-ão registar nos arcos do modelo de Markov os parâmetros relevantes referentes às taxas de avarias e avaliar o sistema para os diferentes tempos de análise pretendidos (Manian *et al*, 1999).

As Árvores de Falhas estáticas expressam os critérios de falha em termos de combinação de acontecimentos, enquanto nas Árvores de Falhas dinâmicas o critério da falha se refere à combinação dos acontecimentos e a sua ordem de ocorrência.

Os Diagramas de Decisão Binária (BDD) não podem ser usados para resolver Árvores de Falhas dinâmicas. Por outro lado, transformar ou converter grandes Árvores de Falhas numa Cadeia de Markov também não é muito prático, uma vez que, tal como referido anteriormente, o tamanho deste modelo aumenta exponencialmente, aumentando também o tempo para encontrar a sua solução.

Uma solução eficiente consiste no uso das duas técnicas de forma equilibrada, usando uma abordagem modular, convertendo uma Árvore de Falhas (FT) para uma MC apenas se existir uma ou mais portas dinâmicas. Se existirem apenas portas estáticas toda a FT é convertida para um BDD.

Na prática, constata-se que apenas uma pequena parte de uma FT é dinâmica por natureza, pelo que a identificação de sub-Árvores independentes nesta abordagem modular promove uma decisão no sentido de cada sub-Árvore ser resolvida com uma das duas técnicas. Estas sub-Árvores são tratadas separadamente e as suas soluções são integradas para posteriormente se obter a solução para toda a FT. Esta abordagem tem a vantagem de reduzir substancialmente qualquer um dos modelos.

A Figura 2.12 ilustra como a metodologia por modularização foi pensada no desenvolvimento do software "Galileo".

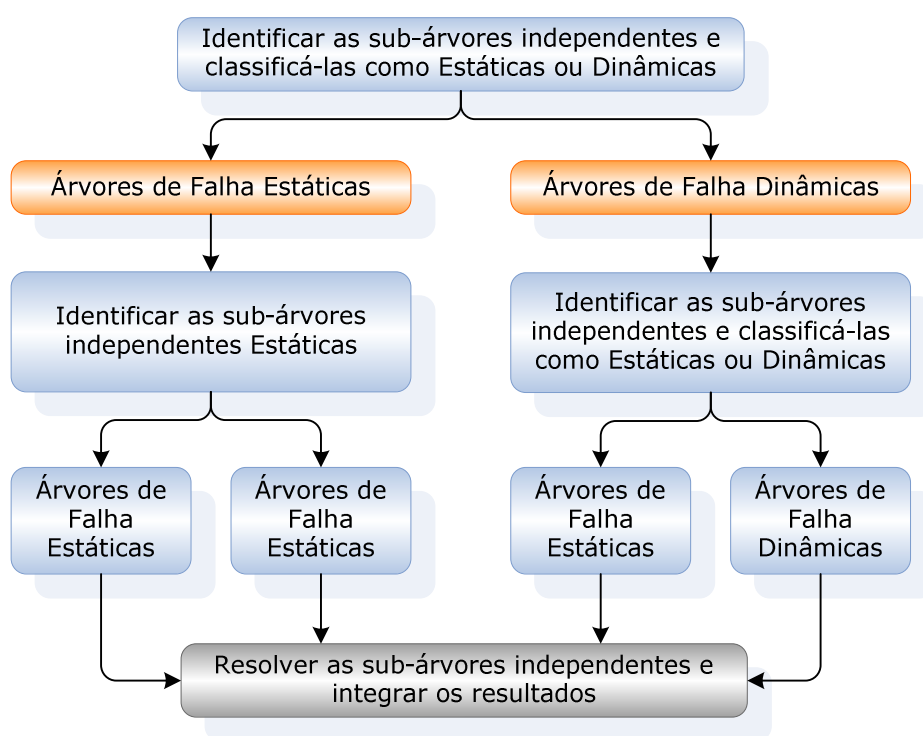
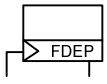



Figura 2.12 – Abordagem modular do software "Galileo"
[Fonte: Galileo® (2004)]

As sub-Árvores independentes são encontradas usando um algoritmo e identificadas como estáticas ou dinâmicas. Desta forma, a etapa mais importante da modulação é encontrar uma forma eficiente de identificar sub-Árvores independentes. Existem vários métodos para detectar estes módulos numa FT, entre os quais se destaca o algoritmo proposto por Dutuit & Rauzy (1996).

Devido ao potencial valor da modulação de Árvores de Falhas dinâmicas, esta metodologia tem vindo a ganhar a atenção dos profissionais da fiabilidade que

normalmente trabalham com sistemas de segurança críticos, não se ficando apenas pelos projectos de investigação. O primeiro passo da metodologia apresentada por Amari *et al* (2003) é idêntico ao apresentado por Gulati & Dugan (1997), ou seja, a identificação dos módulos independentes de uma FT.

De referir que na análise de Árvores de Falhas, as sub-Árvores estáticas podem conter probabilidades de falha constantes (independentes do tempo) ou seguir uma distribuição exponencial, e que as dinâmicas apenas suportam a distribuição exponencial para os tempos para a avaria.

Relativamente às Árvores de Falhas são referidos seis tipos de portas dinâmicas, para além das três portas estáticas (AND, OR e K/N) tradicionais. São elas:

- A porta de dependência funcional (FDEP);
- As portas de sobressalentes *Cold*, *Hot* e *Warm* (CSP, HSP e WSP);
- A porta AND Prioritário (PAND);
- A porta de sequência forçada (SEQ).

A Tabela 2.3 mostra a simbologia de portas lógicas usada em Árvores de Falhas dinâmicas.

Tabela 2.3 – *Portas lógicas dinâmicas*

Símbolo	Descrição
FDEP	Porta lógica "Dependência Funcional" (Gate "FDEP") – Utilizada para indicar que todos os acontecimentos dependentes ocorrem quando o acontecimento despoletador (trigger) ocorre
SP	Porta lógica "Sobressalente (Gate "SPARE") – Utilizada para incluir a utilização de sobressalentes num sistema - O output verifica-se se a falha de todos os sobressalentes ocorrer (Hot Spare / Warm Spare / Cold Spare)
	Porta lógica "E Prioritário" ou "E Sequencial" (Gate "Priority AND") – O output só se verifica se um e outro input se verificarem numa determinada sequência
SEQ	Porta lógica "Sequência Forçada" (Gate "SEQ") – Utilizada para forçar a ocorrência de acontecimentos numa determinada ordem – O output acontece apenas quando todos os inputs ocorrem numa dada ordem (esquerda para a direita)

A porta FDEP é composta por um acontecimento despoletador (ou gatilho) (*trigger*) e um conjunto de componentes dependentes. Quando o acontecimento despoletador ocorre, causa a falha dos componentes dependentes. Através desta porta pode-se representar a ocorrência de falhas simultâneas devido a um acontecimento único. O designado "efeito de dominó" pode ser também representado através de portas FDEP em cascata. A próxima figura mostra uma representação gráfica da porta FDEP.

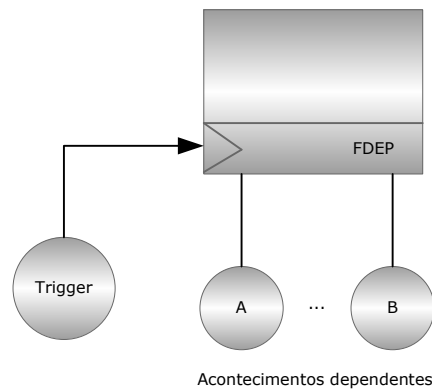



Figura 2.13 – Porta lógica FDEP

Quanto à porta lógica “Spare” pode-se dizer que as portas CSP e HSP são casos particulares da porta WSP, quando os factores de adormecimento (α=*dormancy factors*) correspondem aos valores “0” e “1”, respectivamente. Por exemplo, para a porta CSP com uma entrada primária e uma ou mais entradas alternativas (sobressalentes), onde todas as entradas são acontecimentos básicos (ou componentes), se a entrada primária está inicialmente a funcionar, quando esta falha, é substituída por uma entrada alternativa. A saída da porta CSP é verdadeira (falha) quando a entrada primária e todas as alternativas corresponderem a falhas. A próxima figura mostra também uma representação gráfica deste tipo de porta.

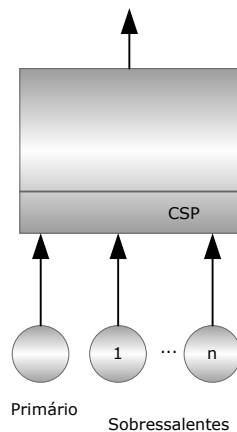



Figura 2.14 – Porta lógica CSP

A porta “E prioritário” (PAND) tem duas entradas (“A” e “B”). O resultado é correspondente a uma falha quando “A” e “B” falham, e desde que “A” falhe antes (ou ao mesmo tempo) de “B”, caso contrário não ocorrerá uma falha.

Com a falha dos dois componentes chega-se a dois estados absorventes, embora um seja de falha do sistema e outro não. A representação gráfica da porta PAND pode ser visualizada através da seguinte figura.

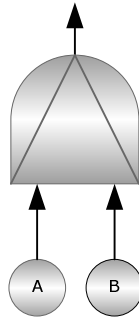



Figura 2.15 – Porta lógica PAND

A porta lógica "Sequência forçada" (SEQ) força as suas entradas a falhar numa ordem sequencial particular, ou seja, só ocorrerá a falha se a sua sequência for respeitada.

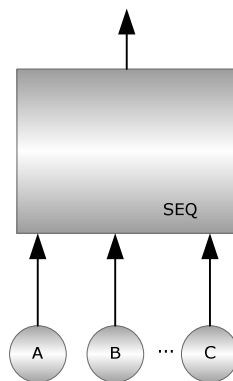



Figura 2.16 – Porta lógica SEQ

2.4 – Conceito de Manutibilidade

O conceito de manutibilidade só deve ser utilizado quando se tratar de bens reparáveis, uma vez que este conceito traduz a facilidade e consequente rapidez com que um bem que avariou ou atingiu a altura de fazer manutenção preventiva pode ser reposto no seu estado operacional.

A manutibilidade do equipamento pode ser definida como a "***Aptidão de um bem, sob condições de utilização definidas, para ser mantido ou restaurado, de tal modo que possa cumprir uma função requerida, quando a manutenção é realizada em condições definidas, utilizando procedimentos e recursos prescritos***" (NP EN 13306, 2007).

A definição de manutibilidade também pode ser dada como a "***capacidade de um item, sob determinadas condições de uso, ser mantido ou restaurado para um estado no qual pode cumprir as funções requeridas, quando a manutenção é realizada em determinadas condições e usando procedimentos e recursos prescritos***" (Rausand & Hoyland, 2004).

Monchy (1996) transcreve a manutibilidade da norma francesa AFNOR X 60-010 como sendo a "***Aptidão de um dispositivo a ser mantido ou restabelecido num estado que possa cumprir a função requerida, em condições de utilização, desde que a manutenção seja realizada em determinadas condições, com os procedimentos e meios prescritos***".

Como se pode observar, as definições anteriores são muito similares. Assim, resumidamente, a manutibilidade de um produto é a sua capacidade, expressa por uma probabilidade, de:

- Ser convenientemente reparado, ou seja, colocar o bem avariado no estado considerado operacional;
- Num período de tempo conveniente;
- Sob condições operacionais e ambientais especificadas;
- Por uma equipa ou operador habilitado.

Claramente, a manutibilidade está relacionada com a fase de projecto do equipamento e com a atenção que nessa fase foi dada a aspectos como:

- ➢ Boa acessibilidade;
- ➢ Montagem das unidades concebida para substituições rápidas;
- ➢ Acesso a inspecções internas por meios alternativos (ex. fibras ópticas);
- ➢ Indicadores de vibração;
- ➢ Identificação dos circuitos pelas cores convencionais;
- ➢ Modularização de funções;

- Utilização de ligas diferentes em zonas e componentes diferentes de modo a permitir pela análise de partículas em suspensão no óleo identificar a sua proveniência, indicando a zona que está a ser afectada por desgaste;
- Outros.

Quando se fala em reparação há que ter o cuidado em separar, de uma forma clara, o que corresponde às acções técnicas de manutenção e o que é inerente a atrasos administrativos ou logísticos (ex.: espera pela chegada de peças sobressalentes).

De acordo com a diversidade de bens e variedade de procedimentos de reparação, os valores da manutibilidade variam de forma significativa, apresentando casos em que a reposição em serviço é praticamente instantânea e outras situações onde se necessita mais tempo.

A manutenção correctiva pode ser quantificada através do tempo médio para reparar (MTTR = *Mean Time To Repair*). No entanto, este tempo inclui diversas actividades, normalmente divididas em três grupos, nomeadamente (O'Connor, 1999):

- Tempo de preparação – encontrar a pessoa para o serviço, deslocação, obter as ferramentas e equipamento de teste, etc…;
- Tempo de manutenção efectivo – tempo exclusivo para fazer a tarefa;
- Atrasos – Tempo logístico, como por exemplo esperar por sobressalentes, uma vez começada a tarefa.

Para Ferreira (1998), os tempos técnicos de reparação (TTR) resultam geralmente do somatório dos seguintes tempos:

- Tempo de verificação que a avaria existe de facto (eliminar o falso alarme);
- Tempo de diagnóstico;
- Tempo de acesso ao orgão avariado;
- Tempo de substituição e/ou reparação;
- Tempo de montagem;
- Tempo de controlo e de arranque do sistema.

Na quantificação da manutibilidade recorre-se normalmente ao indicador correspondente ao tempo médio de reparação ou recolocação em serviço (MTTR), sendo este calculado de uma forma simples para o registo de "n" intervenções através da seguinte expressão.

$$MTTR = \frac{\sum TTR_i}{n} \qquad i = 1,2,3,... \qquad (2.19)$$

Em qualquer estudo que se efectue, convém numa primeira fase especificar de forma correcta o que se entende por *reposição em serviço*, de forma a não influenciar o valor da manutibilidade de forma significativa.

Como a manutibilidade também pode ser traduzida por uma probabilidade, pode-se também ajustar aos tempos de reparação ou recolocação em serviço uma determinada distribuição estatística. À semelhança da fiabilidade, as distribuições estatísticas mais características, quando se efectuam estudos de manutibilidade, são:

- Weibull (1, 2 ou 3 parâmetros);
- Exponencial (1 ou 2 parâmetros);
- Lognormal (2 parâmetros);
- Normal (2 parâmetros).

Também de forma análoga aos estudos de fiabilidade, quando se fala no conceito de manutibilidade, pode-se referir a função densidade de probabilidade de reposição [g(t)]. A função manutibilidade corresponde à probabilidade do tempo para recolocação em serviço ser inferior a um dado tempo "t". Desta forma, a função manutibilidade pode ser expressa por:

$$M(t) = \Pr(TTR < t) \qquad t > 0 \qquad (2.20)$$

ou

$$M(t) = \int_0^t g(t)dt \qquad (2.21)$$

A Figura 2.17 mostra o comportamento típico da variação deste tipo de curvas no tempo, de acordo com os parâmetros da distribuição em causa.

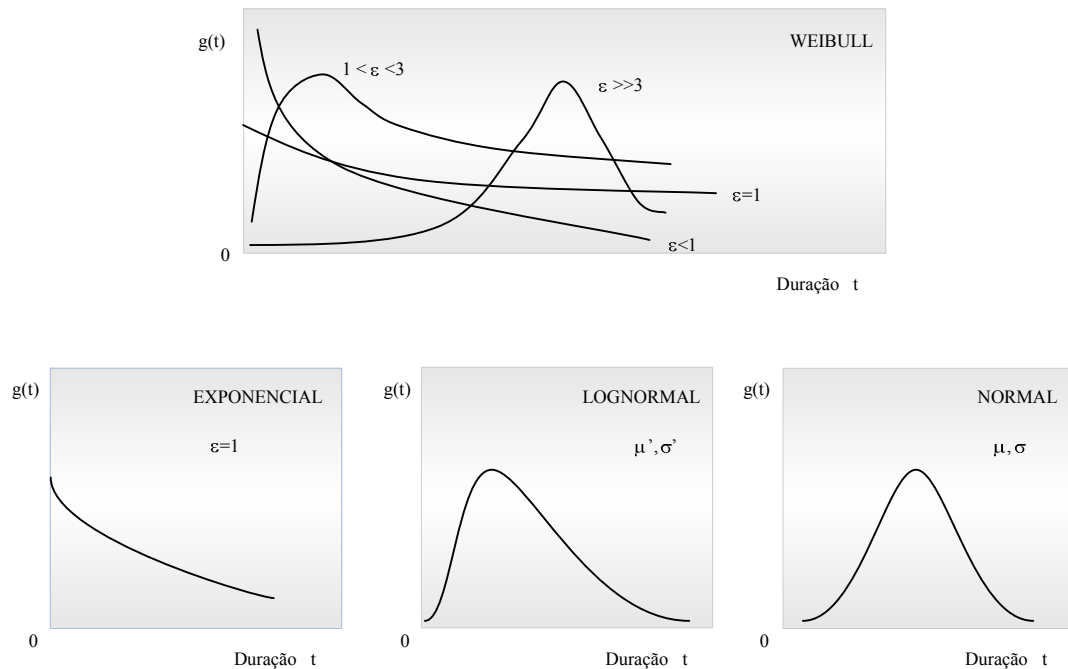



Figura 2.17 – Tipos mais comuns da função densidade de probabilidade de reposição

A distribuição de Weibull é de uma forma geral muito prática, uma vez que pode englobar a maioria dos casos práticos, tudo devido à influência do parâmetro de forma (ε). A distribuição Exponencial pode ser considerada um caso particular da distribuição de Weibull, onde o parâmetro de forma assume o valor unitário (ε = 1).

A distribuição Normal aplica-se quando as reposições em serviço se concentram em torno de um valor médio de forma simétrica. Esta distribuição assemelha-se com a distribuição de Weibull quando o parâmetro de forma (ε) assume valores próximos de 3,4.

É a distribuição que mais frequentemente se utiliza em estudos de manutibilidade, uma vez que a maior parte dos trabalhos de recolocação em serviço se efectua à volta de valores considerados tempos-padrão.

Além destas distribuições mais usuais, outras poderão corresponder aos dados relativos às recolocações em serviço, como a distribuição Gama, Gama Generalizada ou Logística, entre outras, embora não aconteça com tanta frequência.

2.5 – Conceito de Disponibilidade

De acordo com a norma portuguesa NP EN 13306 (2007), disponibilidade é a "***Aptidão de um bem para cumprir uma função requerida sob determinadas condições, num dado instante ou durante um dado intervalo de tempo, assumindo que é assegurado o fornecimento dos necessários recursos externos***", com uma nota mencionando que esta aptidão depende da combinação da fiabilidade, da manutibilidade e da adequabilidade da manutenção.

A disponibilidade também pode ser descrita como a "***capacidade de um item (sob determinados aspectos combinados de fiabilidade, manutibilidade e suporte de manutenção) realizar a função requerida num dado instante ou durante um dado período de tempo***" (Rausand & Hoyland, 2004).

O complementar da disponibilidade [$A(t)$] é a indisponibilidade [$Q(t)$], satisfazendo a relação:

$$A(t) + Q(t) = 1 \tag{2.22}$$

Poder-se-ia numa primeira fase afirmar que a disponibilidade depende basicamente de:

- Frequência de avarias – Fiabilidade;
- Tempo de reparação das avarias (bens reparáveis) – Manutibilidade

No entanto, existem outros factores que não devem ser esquecidos, tais como:

- Tipo e frequência de intervenções – Estratégia de manutenção;
- Quantidade e qualidade dos meios administrativos e logísticos, e sua interdependência – Logística.

A Figura 2.18 mostra as relações entre a disponibilidade, a manutibilidade e a fiabilidade para bens reparáveis.

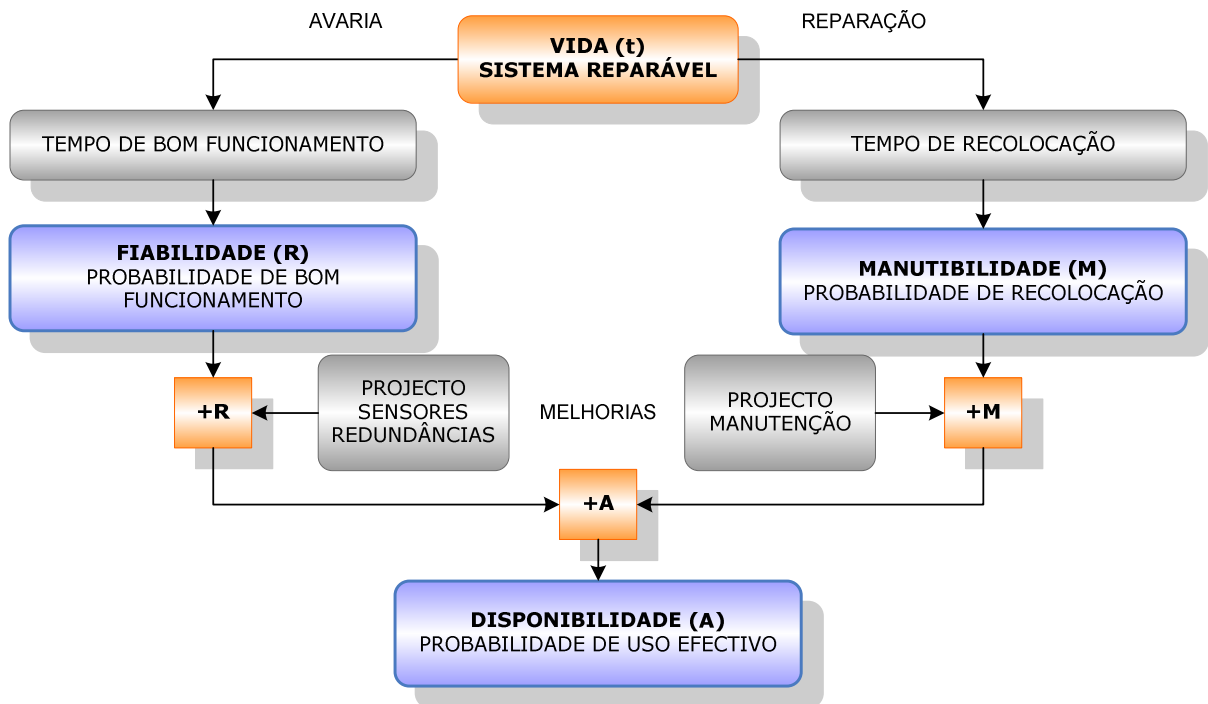



Figura 2.18 – Relação entre Disponibilidade, Manutibilidade e Fiabilidade
[Fonte: Pallerosi (2007d)]

A afirmação corrente de que quando se analisam bens não reparáveis o conceito de fiabilidade se torna um caso particular da disponibilidade, assumindo desta forma valores idênticos é discutível, e é necessário definir bem o que está em causa. Esta ideia pode ter algum fundamento quando analisada do ponto de vista da disponibilidade do bem, mas quando observada a disponibilidade em termos da função, tendo em conta os tempos referentes à troca do bem avariado por outro, com as inerentes acções de pesquisa da avaria, acesso ao local, disponibilização de mão de obra, etc., a fiabilidade e a disponibilidade (funcional) do equipamento ou sistema não terão obrigatoriamente os mesmos valores. De acordo com a representação da Figura 2.18, constata-se que o aumento da disponibilidade é alcançado se a fiabilidade e/ou a manutibilidade forem melhoradas. De facto, ao reduzir-se a probabilidade de avaria e/ou ao se diminuirem os tempos de intervenção para realizar as actividades de manutenção, quer de carácter preventivo, quer correctivo, o tempo global em que o bem se encontra disponível para cumprir a sua função aumentará. No entanto, a disponibilidade (ou indisponibilidade) pode ser referida a várias condições e durações de referência, podendo ser apresentada de várias formas. Os próximos parágrafos descrevem os vários tipos de disponibilidade.

2.5.1 – Disponibilidade instantânea

A disponibilidade instantânea é a probabilidade de um bem ser capaz de desempenhar uma função requerida, sob dadas condições, num dado instante, supondo-se que os recursos externos estão assegurados.

Quando se trata de variáveis contínuas, para o cálculo da disponibilidade instantânea de um sistema adopta-se uma solução numérica, por meio de simulação, com recurso a software disponível devido à complexidade das soluções analíticas (diferentes distribuições estatísticas para os componentes do sistema para a fiabilidade e manutibilidade). Quanto maior o número de simulações, maior o tempo requerido para os cálculos, mas melhor a precisão dos resultados (se as simulações forem as mais correctas).

No caso de nos referirmos a bens reparáveis (uma unidade simples) com taxa de avarias (λ) e taxa de reparação (μ) constantes, a disponibilidade instantânea, ou probabilidade do bem se encontrar disponível no tempo "*t*" é igual a (O'Connor, 1999):

$$a(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\lambda + \mu}.e^{[-(\lambda+\mu).t]} \qquad (2.23)$$

2.5.2 – Disponibilidade média

A disponibilidade média pode ser descrita como a média das disponibilidades instantâneas durante um determinado intervalo de tempo.

Para variáveis contínuas, e de forma análoga ao cálculo da disponibilidade instantânea, adopta-se uma solução numérica, por meio de simulação, com recurso a software disponível. Nota-se uma tendência decrescente dos valores pontuais da disponibilidade, desde "t=0", tendendo assimptoticamente para um determinado valor. A disponibilidade média calcula-se fazendo tender para infinito o valor "t" da expressão (2.23).

$$A(t) = \lim_{t \to \infty} a(t) \qquad (2.24)$$

No caso particular, onde a taxa de avarias (λ) e taxa de recolocação (μ) são constantes, correspondentes a modelos de distribuição exponenciais, a disponibilidade média (ou assimptótica), é dada por:

$$A(t) = \frac{\mu}{\mu + \lambda} \tag{2.25}$$

Ou, em função das durações, na forma:

$$A(t) = \frac{MUT}{MUT + MDT} \tag{2.26}$$

com

MUT = Tempo médio de funcionamento (*Mean Up-Time*)

MDT = Tempo médio de paragem (*Mean Down-Time*)

De acordo com Pallerosi (2007d), consegue-se determinar o valor assimptótico da disponibilidade para durações correspondentes a cerca de 4 (quatro) vezes o valor do tempo médio até à falha (MTTF).

O valor da disponibilidade média (ou assimptótica) é um dado importante, pois na prática define a disponibilidade real de um bem durante um longo período de utilização, característico da sua qualidade de exploração e manutenção.

Por vezes a disponibilidade média também é referida como a disponibilidade inerente (ou intrínseca), que se refere ao tempo médio até à avaria e ao tempo médio até à recolocação, não incluídos os atrasos logísticos e administrativos nas reparações. Esta é uma expressão muito comum quando se pretende quantificar a disponibilidade, embora seja mais aplicável a bens reparáveis.

$$A(t) = \frac{MTTF(MTBF)}{MTTF(MTBF) + MTTR} \tag{2.27}$$

É importante realçar que quando se trata de equipamentos novos, com as inerentes avarias no período inicial de operação (ver 2.3.2), período onde as taxas de avaria são decrescentes, haver a possibilidade de se verificar uma disponibilidade crescente com o uso, contrariando um pouco as explicações dos parágrafos anteriores. Será então

necessário proceder-se a uma análise independente da disponibilidade após este período (período de mortalidade infantil).

Deve-se também considerar a situação de se poderem verificar reparações imperfeitas, havendo em determinados cálculos a hipótese de afectar o bem de um factor de restauração. A política de recursos humanos também deve ser tida em conta, uma vez que em determinados casos a disponibilidade e o nível de formação do pessoal para efectuar a manutenção podem induzir atrasos recorrentes nas acções a realizar.

A fórmula de cálculo da disponibilidade média varia de acordo com o tipo de arranjo em que os componentes que fazem parte desse sistema se encontram (O'Connor, 1999). A expressão (2.28) refere-se ao cálculo de um sistema com "n" componentes idênticos em série.

$$A(t) = \prod_{i=1}^{n} \frac{\mu_i}{\lambda_i + \mu_i} \qquad (2.28)$$

No caso de "n" componentes idênticos em paralelo activo, a disponibilidade média é determinada pela seguinte expressão:

$$A(t) = 1 - \prod_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \mu_i} \qquad (2.29)$$

Para um sistema "k/n", como por exemplo um sistema "2 em 3", a disponibilidade média pode ser determinada através da expressão (2.30).

$$A(t) = 1 - \frac{1}{(\lambda + \mu)^n} . \sum_{i=0}^{k-1} \binom{n}{i} \mu . \lambda^{n-i} \qquad (2.30)$$

Conforme se pode constatar, na eventualidade de os componentes não serem idênticos ou quando se trata de sistemas complexos, será necessário recorrer a programas informáticos especializados para se determinar a sua disponibilidade média.

2.5.3 – Disponibilidade operacional

A disponibilidade operacional considera todos os tempos adicionais para recolocação do bem no estado funcional, tais como os tempos indisponíveis devido a manutenção preventiva e atrasos logísticos ou administrativos, reflectindo o seu valor não só as características de fiabilidade e manutibilidade, como também os aspectos organizacionais e operacionais.

Representa o valor da disponibilidade correspondente à utilização real do bem após a ocorrência de falhas e recolocações. Quando se tenta estimar este valor, tem que se ter em conta a dificuldade em controlar alguns tempos adicionais, uma vez que os mesmos apresentam uma grande variação, devido fundamentalmente a factores externos (fornecimento de bens ou serviços).

2.6 – Conceito de Segurança

De acordo com a MIL-STD 882-C (1993), segurança é definida como a "***Ausência das condições que podem causar morte, ferimentos, doença, dano ou perda de equipamento ou propriedade, ou dano para o ambiente***".

O conceito de segurança está intimamente ligado aos outros três elementos do RAMS já referidos, fundamentalmente quando falamos de aplicações consideradas críticas ou instalações de alto risco industrial, se com a ocorrência de avarias ou indisponibilidade dos equipamentos estiverem em causa riscos para a vida humana, ambiente ou factores económicos relacionados com a perda de bens ou cessação das actividades. Dizemos que existe segurança quando há ausência de risco não aceitável (NP EN 50126, 2000).

Para toda a aplicação crítica em termos de segurança deverão adoptar-se mecanismos especiais, de forma a garantir que qualquer estado considerado inseguro não ocorra. Se tal acontecer, o sistema deverá promover uma redução ou mitigação das suas consequências e a rápida recuperação para um dado estado considerado seguro.

Como exemplos mais marcantes, podem-se referir as instalações nucleares, sistemas de transportes aéreos ou ferroviários, equipamentos médicos e a área da energia, entre outros. Neste último caso, a energia eléctrica toma carácter de relevo, uma vez que dela

dependem inúmeros sistemas críticos, onde uma falha de energia pode ter efeitos graves (ex. hospitais, sinalização rodoviária).

Normalmente as aplicações críticas ou de alto risco quanto à segurança estão sujeitas a regulamentação rígida, garantindo assim que a preocupação com a segurança esteja presente desde o projecto, desenvolvimento e implementação do sistema, assim como na fase de exploração (manutenção) e em alguns casos na fase de abate ou desmantelamento.

O desenvolvimento de soluções tecnológicas, que restringem ou reduzem a possibilidade de avaria nos sistemas, e neste caso com maior incidência nos sistemas críticos ou de alto risco, torna-se um grande desafio no campo da investigação e engenharia.

A maioria das aplicações necessita de um sistema de supervisão e controlo de forma a garantir que os requisitos especificados sejam cumpridos. Este sistema de supervisão e controlo deverá também merecer especial atenção, uma vez que dele dependem os sistemas supervisionados.

Sempre que um bem se encontra a desempenhar as suas funções de segurança nas condições estabelecidas e durante um período de tempo determinado, designa-se por integridade da segurança. De acordo com normas internacionais (IEC 61508, 1998) estabelecem-se níveis discretos de integridade de segurança (SIL = *Safety Integrity Level*) para especificar os requisitos das funções de segurança. Ao nível de integridade de maior valor (SIL 4) corresponde o nível de integridade de segurança mais elevado.

Os conceitos técnicos de segurança são baseados no conhecimento de (NP EN 50126, 2000):

- Situações potencialmente perigosas do sistema;
- Característica de cada situação potencialmente perigosa, quanto à gravidade das suas consequências;
- Critérios de falha contrários à segurança (modos de falha, probabilidade de ocorrência, sequência ou coincidência de acontecimentos, estados operacionais, condições, etc.);
- Manutibilidade dos bens (facilidade para executar manutenção, probabilidade de ocorrência de erros durante as acções de manutenção, tempo para se atingir um estado de segurança, etc.);

- Sistema de exploração e manutenção (influência de factores humanos, ferramentas, infra-estruturas logísticas, procedimentos e controlos, etc).

A segurança, como um elemento de extrema importância nas instalações industriais de risco elevado, pode ser salvaguardada com recurso à introdução de factores de segurança na fase de projecto, com base em estudos probabilísticos referentes aos modos de falha, ou com ambos os critérios, como é o caso da metodologia FPSF (*Failure Probability-Safety Factor Method*) que combina os constrangimentos referentes aos factores de segurança e a probabilidade de falha (Castillo *et al*, 2003). Neste aspecto particular, os factores de segurança surgem em muitos casos associados à fiabilidade, mostrando a existência de uma relação entre ambos os conceitos (Ching, 2009). Burdekin (2007) explica os princípios gerais para aplicar os referidos factores de segurança na fase de projecto e nos estudos de integridade estrutural.

Em alguns estudos de segurança dá-se mais ênfase à própria sequência dos acontecimentos que levam à falha do sistema e às probabilidades de ocorrência dessa sequência do que propriamente ao conhecimento dos modos de falha dos componentes (Adamyan & He, 2002). Nesta perspectiva, a Figura 2.19 retrata uma Árvore de Acontecimentos para o exemplo já mencionado aquando da referência à Análise de Árvore de Falhas (FTA).

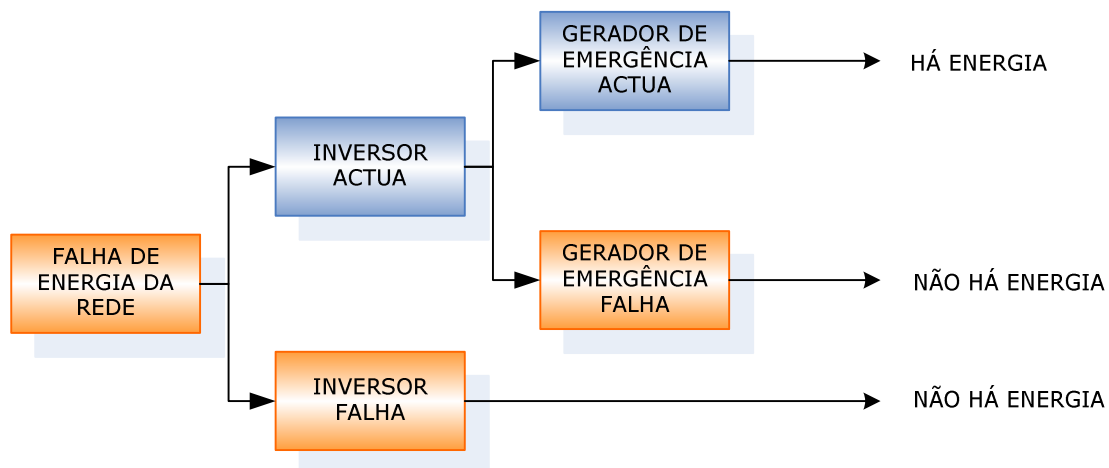



Figura 2.19 – Exemplo de uma Análise de Árvore de Acontecimentos

Os resultados numéricos dos estudos probabilísticos de segurança (PSA = *Probabilistic Safety Assessment*) dependem da informação ou dados relativos à fiabilidade e dos métodos usados na análise.

Hauptmanns (2009) mostra no seu trabalho como os resultados variam quando se dispõe de conjuntos de dados distintos e se opta por diferentes critérios de sucesso para os sistemas de segurança de uma instalação. O mesmo autor mostra noutro estudo (Hauptmanns, 2008) o impacto dos dados de fiabilidade nos cálculos probabilísticos de segurança. De facto as bases de dados de fiabilidade, assim como a informação referente às taxas de avarias, podem servir de ponto de partida para uma melhoria da segurança (Keren *et al*, 2003).

Sorensen (2002) mostra numa interessante compilação a evolução do termo "*cultura de segurança*" e a relação entre cultura de segurança e a segurança das operações na produção de energia nuclear e outras tecnologias potencialmente perigosas. Segundo este autor, os atributos de uma cultura de segurança incluem uma boa organização das comunicações e da formação e uma gestão empenhada na temática da segurança, o que permite reduzir erros latentes em sistemas complexos.

Como não podia deixar de ser, a segurança de equipamentos e instalações está em grande parte associada aos erros humanos. Colombo & Demichela (2008) propõem uma metodologia de integração do desempenho e dos resultados das análises de fiabilidade humana (HRA = *Human Reliability Analysis*) em estudos de risco quantitativos (QRA = *Quantitative Risk Assessment*), e nomeadamente dos factores humanos e organizacionais em análises de segurança. Outro estudo demonstra os benefícios de usar os factores humanos na melhoria da segurança dos sistemas e da fiabilidade dos mesmos (Hughes & Kornowa-Weichel, 2004).

Como se pode constatar através dos parágrafos anteriores, o conceito de segurança encontra-se directamente ligado à noção de risco. De facto, o risco torna-se um tema inevitável quando se efectuam as mais diversas análises de instalações industriais de risco elevado. Se teoricamente nestas instalações não existissem quaisquer tipos de risco (vida humana, económicos, ambientais), não se justificaria a realização de estudos na área do RAMS.

Assim, devido à importância demonstrada na questão do **risco**, justifica-se a introdução do Capítulo III, exclusivamente dedicado a esta temática.

2.7 – Conclusões do Capítulo

Neste capítulo fez-se uma introdução ao conceito RAMS (*Reliability*, *Availability*, *Maintainability and Safety*), mostrando a sua importância no contexto industrial e a sua aplicação ao longo de todo o ciclo de vida dos bens e suas implicações no risco. Foi referida a importância da Fiabilidade e da Manutibilidade na Disponibilidade e na Segurança operacional. Conceptualmente, na metodologia RAMS, os dois primeiros factores podem ser referenciados como factores originais (ou de *input*), enquanto os dois últimos factores como resposta (ou *output*).

Para melhor compreensão de cada um dos referidos elementos do RAMS, foram apresentadas individualmente as suas características e alguns conceitos relacionados com cada uma das temáticas.

Relativamente à **Fiabilidade**, foram apresentadas algumas definições e apontadas algumas razões que justificam o seu estudo. Mostraram-se as principais diferenças entre os conceitos de fiabilidade e qualidade com a introdução da fiabilidade como uma extensão da qualidade ao longo do tempo. Relativamente às estimativas da fiabilidade foram referidas as duas fontes onde fundamentalmente nos podemos basear para prever a fiabilidade dos bens, nomeadamente a execução de ensaios ou o recurso a bases de dados.

Quanto aos ensaios foram ainda referidos os vários tipos de ensaios normalmente realizados para determinação ou cálculo da fiabilidade, como os ensaios normais, ensaios acelerados (ALT) ou os ensaios altamente acelerados (HALT), assim como os seus objectivos e aplicações típicas.

Foi explicada a noção de bem reparável e bem não-reparável (descartável), acentuando as suas diferenças e a distinção na abordagem quando se realizam estudos de fiabilidade. Apesar de não se proceder ao seu desenvolvimento no presente trabalho, tornou-se imperioso referir o tema da fiabilidade humana e algumas metodologias actualmente usadas no cálculo deste factor, que em muitas situações pode ser a principal fonte de ocorrência de acidentes. Referiram-se as avarias de causa comum (CCF) como algo a ter em conta nas análises de fiabilidade, uma vez que a sua ocorrência também poderá ter grande influência nos resultados obtidos.

Referiram-se também outros conceitos relacionados com a fiabilidade, como por exemplo a distinção entre falha e avaria e entre acontecimentos dependentes e independentes. Foram referidas as principais funções associadas ao cálculo da fiabilidade, como a função densidade de probabilidade de falha, fiabilidade e probabilidade acumulada de falha, assim como taxa de avarias, tempo médio de vida e fiabilidade condicional.

Ainda dentro do estudo de fiabilidade foi referida a importância do cálculo da fiabilidade de componentes e apresentadas no **Anexo I** as principais distribuições estatísticas mais em pormenor. No seguimento deste tema remeteu-se para o **Anexo IV** o cálculo da fiabilidade de sistemas, de acordo com o tipo de arranjo em que os componentes que os constituem se encontram (série, paralelo, *standby*, k/n, etc.).

Para o cálculo da fiabilidade descreveram-se alguns métodos como a Árvore de Acontecimentos, os diagramas de Blocos de Fiabilidade, as Redes de Petri e as Árvores de Falhas. Neste aspecto em particular aprofundou-se a metodologia de Análise de Árvores de Falhas, distinguindo as Árvores estáticas das dinâmicas e apresentando as razões que levaram a evoluir das primeiras para as últimas.

O segundo factor explicado em detalhe foi o conceito de **Manutibilidade**. Neste tema, partiu-se da sua definição e da tradução da manutibilidade como uma probabilidade. Verificaram-se alguns aspectos e características que se devem ter em conta na fase de projecto com vista à melhoria da manutibilidade e mostrou-se neste contexto a diferença entre o que propriamente se entende como acções técnicas de manutenção e questões como atrasos logísticos ou administrativos. Desta forma, aproveitou-se para demonstrar que relativamente aos tempos de recolocação em serviço de um determinado bem, também se podem ajustar as distribuições estatísticas usadas nos estudos de fiabilidade.

O terceiro conceito a ser referido foi a **Disponibilidade**, descrevendo como este é fortemente influenciado pelos dois conceitos anteriores (Fiabilidade e Manutibilidade). Apresentaram-se alguns tipos de disponibilidade e a forma como os mesmos podem ser calculados.

De forma a completar em detalhe todos os elementos do RAMS, passou-se ao último conceito, relacionado com a **Segurança**. Neste aspecto, tornou-se imperioso referir a noção de risco como ideia complementar à segurança, abrindo espaço para o próximo tema. Assim, este capítulo serviu para apresentar e cimentar as bases para o trabalho realizado, sendo fundamental para a compreensão dos próximos capítulos.

CAPÍTULO III

RISCO

3.1 – Introdução

Qualquer actividade integra nos seus mais variados aspectos uma análise e uma gestão dos riscos. Independentemente das situações, quer se trate de questões pessoais, profissionais ou até mesmo governativas, existe uma necessidade constante para a tomada de decisões onde normalmente o risco é ponderado, muitas vezes sem a sua percepção.

Outras decisões, porém, carecem de uma análise mais profunda e maior ponderação quanto à opção a escolher. Como qualquer acontecimento depende de um conjunto de factores, existe sempre uma incerteza associada, o que torna a tomada de decisões uma tarefa por vezes complicada pois é necessário avaliar essas incertezas. Trata-se de um processo onde se estima o risco envolvido em cada opção, seguido de uma avaliação e tomada de decisão pela opção mais favorável, assumindo o risco ou, por vezes, transferindo-o para terceiros (ex. seguros). A aceitação do risco tem normalmente a ver com o que se considera serem os valores máximos admissíveis para cada situação específica.

A primeira definição conhecida de risco citada na literatura aparece na obra "*Logic, or the Art of Thinking*" (Arnauld & Nicole, 1996) publicada pelo *Port Royal Monastery*, em Inglaterra, no ano de 1662, onde risco é definido como sendo: "***O medo do dano (harm), que deverá ser proporcional não só à gravidade do dano mas também à probabilidade de ele acontecer***".

A noção de risco e a sua percepção pelo público tem evoluído com o tempo. No entanto, a avaliação matemática do risco é relativamente recente. Só em meados do séc. XX é que se desenvolveram as ferramentas matemáticas necessárias para um tratamento científico mais rigoroso deste problema. Quando os riscos são identificados e avaliados pode-se então considerar se são aceitáveis ou não. É obvio que esta tomada de decisão deve ser feita dentro de pressupostos realistas e objectivos de segurança para pessoas, ambiente e bens.

Qualquer que seja a área estudada, quer seja nuclear, aeroespacial, química, automóvel ou outra, a segurança tem vindo a ganhar cada vez mais importância. Segundo Kumamoto (2007), de acordo com as actividades internacionais desenvolvidas nesta área, transformou-se este século numa era de prioridade à segurança (*safety-first age*). Em termos de risco, são estabelecidos objectivos e a partir daí desenvolvem-se projectos, instalam-se os equipamentos e procede-se à sua exploração, nunca esquecendo a manutenção dos mesmos.

A falha é um fenómeno inevitável em todos os produtos e sistemas tecnológicos. Do ponto de vista científico e da engenharia, a investigação do incerto e obscuro domínio das falhas leva à exploração dos limites funcionais e físicos dos sistemas, no esforço de perceber como, porquê e quando um bem não irá funcionar adequadamente. Seja qual for o contexto, o controlo e gestão das falhas é fundamental na gestão do risco.

Tal como já referenciado no capítulo anterior, as áreas relacionadas com a análise das falhas tornam-se multidisciplinares, uma vez que envolvem temas como a fiabilidade, disponibilidade, manutibilidade e segurança (RAMS), risco, qualidade, detecção, identificação de falhas e tolerância à falha, entre outras.

3.2 – Risco

Pode-se começar por definir o que é o risco. Fundamentalmente, o risco envolve acontecimentos futuros de consequências incertas e pretende quantificar o que se espera a nível de consequências. Assim, "***o risco é basicamente composto por duas componentes, uma é a incerteza quanto à ocorrência dos acontecimentos futuros e a outra refere-se à dimensão ou intensidade das consequências de cada acontecimento possível***" (Rausand & Hoyland, 2004). Esta é a definição clássica do risco.

Tipicamente, quando se fala em risco relacionam-se as duas componentes anteriormente referidas com aspectos como a vida humana, valores materiais ou consequências ambientais. Por vezes, conseguimos relacionar com valores monetários, traduzindo o risco em valores mais palpáveis e fáceis de analisar.

Henley & Kumamoto (1981) referem o risco como "***a probabilidade de perda ou danos para as pessoas e propriedade***". Neste conceito, um dos objectivos de uma análise de risco passa pela atribuição de uma frequência (probabilidade) às consequências possíveis para a avaria de um sistema (ex.: *o número expectável de vitimas por ano devido à explosão de um reactor é* 10^{-4}). Nesta vertente, Farmer apresentou nos anos 60 uma relação entre a dimensão estimada de uma fuga radioactiva para a atmosfera motivada por um acidente num reactor nuclear e a probabilidade de ocorrência desse acidente específico, definindo graficamente uma linha limite para a frequência de fuga radioactiva que poderia ser utilizada posteriormente como um guia para novas instalações ou para a avaliação da segurança das instalações existentes. A partir deste tipo de abordagem surgiram diversas aplicações, dando origem às designadas "curvas de Farmer".

Convém não esquecer outro factor importante no risco, que é a dimensão tempo. Normalmente as probabilidades variam com o tempo de exposição a uma dada situação. Assim, a definição mais precisa do risco pode ser expressa pelo valor esperado, por unidade de tempo, das consequências de determinado processo. Pode-se afirmar que o risco é uma combinação da probabilidade de dano e a sua severidade, enquanto a segurança se relaciona com a ausência de risco considerado inaceitável.

3.2.1 – Análises de Risco

Na análise de risco de um processo ou sistema pretendem-se fundamentalmente determinar os riscos a que o mesmo está sujeito. A análise de risco pode ser qualitativa ou quantitativa. Normalmente uma análise quantitativa pressupõe inicialmente uma abordagem qualitativa, que posteriormente é quantificada de acordo com as informações recolhidas sob o processo ou sistema em causa.

A primeira etapa é constituída por um processo de identificação dos potenciais perigos que podem levar à ocorrência de acidentes. Esta fase deve ser levada a cabo por uma

equipa multidisciplinar constituída por pessoas operacionais do terreno, responsáveis pela manutenção, especialistas em análise de risco e gestão, entre outros.

Após esta fase passa-se à identificação das sequências de acontecimentos que os potenciais perigos anteriormente identificados podem originar, assim como, os acontecimentos finais dessas sequências. Entre as várias técnicas disponíveis salienta-se a Árvore de Acontecimentos (ETA = *Event Tree Analysis*) e a Árvore de Falhas (FTA = *Fault Tree Analysis*), ambas já referidas no Capítulo II.

Normalmente, a Árvore de Falhas é usada para calcular a probabilidade de ocorrência de um dado acontecimento e a Árvore de Acontecimentos para determinar a probabilidade das várias consequências possíveis desse mesmo acontecimento.

Outra ferramenta normalmente utilizada é a técnica HAZOP (*Hazard and Operability*), que considera desvios aos atributos dos objectos. Estes atributos incluem quantidades físicas como caudais, temperaturas, pressões, concentrações, forças, tempos, etc. A técnica HAZOP utiliza determinadas palavras-guia para especificar acontecimentos anormais, tais como "não", "mais", "menos", "antes" e "depois", entre outras.

Posteriormente, as causas relativas aos desvios assinalados são também investigadas. No trabalho apresentado por Kumamoto (2007) pode-se analisar uma lista do vocabulário usado para expressar os referidos acontecimentos anormais ou desvios.

A utilização de métodos quantitativos surgiu durante a segunda guerra mundial, para resolução de problemas estratégicos e tácticos, tendo outros investigadores continuado a aplicação de métodos quantitativos noutras áreas que não a militar. Os métodos quantitativos são especialmente úteis em sistemas complexos de grande dimensão, onde seria difícil de resolver apenas com base na experiência ou intuição. Também é indicado para abordagens a problemas novos que possam surgir, ajudando na tomada de decisão.

De acordo com a IEC 60300-3-9 (1995) uma análise de risco corresponde ao "***Uso sistemático de informação disponível para identificar perigos e estimar o risco para indivíduos ou populações, propriedade ou ambiente***".

De acordo com a NS 5814 (1991), será "***Uma aproximação sistemática para descrever e/ou calcular o risco. A análise de risco envolve a identificação de***

acontecimentos indesejados e as causas e consequências desses acontecimentos".

Relativamente a análises de risco, podem-se referir os seguintes documentos:

- **IEC 60300-3-9 –** "*Risk analysis of technological systems*"
- **EN 1050** – "*Safety of machinery – risk assessment*"
- **EN 50126 –** "*Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*"
- **ISO 17776 –** "*Petroleum and natural gas industries – Offshore production installations – Guidelines and tools for hazard identification and risk assessment*"
- **Norsok Z-013 –** "*Risk and emergency preparedness analysis*"
- **EN 1441 –** "*Medical Devices – Risk Analysis*"

As análises de risco, propriamente ditas, iniciaram-se a partir dos anos 60 na indústria nuclear, com avaliações probabilísticas (PRA - *Probabilistic Risk Assessment*), seguindo-se estudos similares a partir dos anos 70 na indústria química, quantificando o risco (QRA - *Quantitative Risk Assessment*) e dando origem à Directiva Seveso (I e II).

Embora em termos gerais se mencione o risco relacionado com um determinado modo de falha, referindo a sua probabilidade de ocorrência e a gravidade das suas consequências, pode-se falar em análise de risco, para uma determinada actividade, verificando o risco global através de uma listagem de todas as suas potenciais consequências e as correspondentes probabilidades associadas (Rausand & Hoyland, 2004). Normalmente, apenas as consequências indesejáveis são consideradas. Quantitativamente, e com base no anteriormente descrito, o risco é por vezes definido como:

$$Risco = C_1 p_1 + C_2 p_2 + ... + C_k p_k = \sum_{i=1}^{k} C_i p_i \quad (3.1)$$

onde:

C_i = Consequência tipo i

p_i = Probabilidade de ocorrência da consequência tipo i

A expressão anterior requer que todas as consequências sejam consideradas com uma medida comum (ex. valor monetário). Na Figura 3.1 pode ser visualizado um esquema referente à metodologia genérica de uma análise de risco quantitativa.

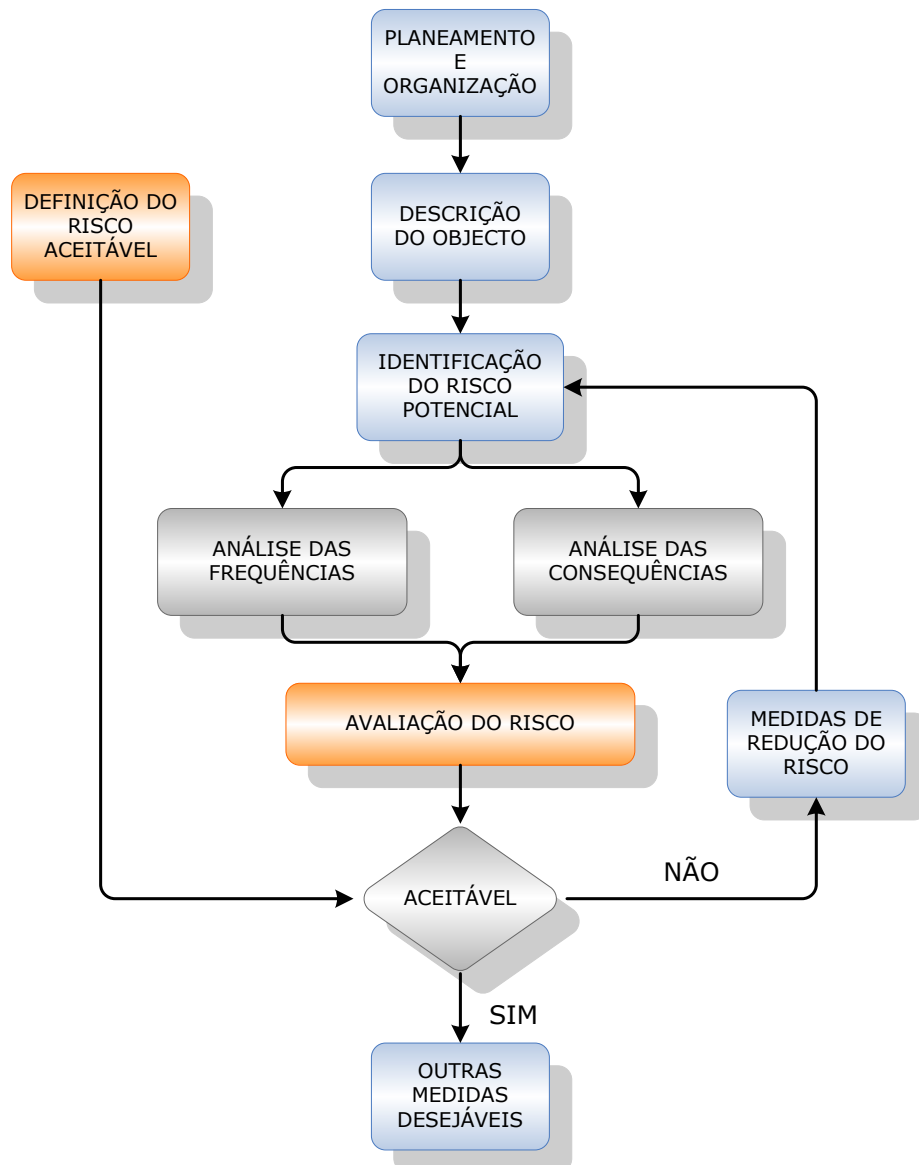



Figura 3.1 – Metodologia de Análise de Risco quantitativa
[Fonte: Rausand & Hoyland (2004)]

A interpretação do esquema referente à metodologia genérica de análise de risco quantitativa é efectuada nos parágrafos seguintes.

Planeamento e organização – Nesta fase inicial pretende-se:

- Identificar a legislação e regulamentos relevantes;
- Clarificar políticas internas e critérios de aceitação do risco;
- Definir o objectivo da análise de risco – Que tipos de risco devem ser estudados? (grandes acidentes vs. acidentes ocupacionais, perigos aleatórios, acções deliberadas e/ou cargas ambientais) – que fases do ciclo de vida devem ser incluídas? (operação normal, arranque, fim de vida, revisões gerais, etc.);

- Organizar o trabalho através de uma equipa multidisciplinar, onde especialistas dão a sua sabedoria.

Descrição do objecto de análise - A descrição envolve tudo o que possa influenciar os resultados da análise. As questões principais são:

- De que é que o sistema é dependente? (*inputs*)
- Que actividades são realizadas pelo sistema? (funções)
- Que serviços fornece o sistema? (*outputs*)
- Relações técnicas, pessoais e organizacionais;
- Relações políticas, sociais e económicas significantes;
- Associação e dependência com o exterior;
- Apoio externo se ocorrer um acidente;
- Indicar relações especiais que sejam significativas para a segurança.

Grandes instalações podem eventualmente ser repartidas em pequenos elementos (objectos e/ou funções). Alguns aspectos devem ser tidos em consideração, nomeadamente ter a noção que uma estratificação que inclua muitos e pequenos elementos necessita de muitos recursos, e que uma estratificação insuficiente pode levar a omissões não intencionais de acontecimentos raros, mas significantes. Uma técnica possível de efectuar para repartir um sistema é por exemplo através da estratificação hierárquica.

Identificação dos perigos – Nesta fase os perigos potenciais relacionados com a actividade devem ser identificados (perigos mecânicos, incêndio, explosão, materiais tóxicos, radiação, etc.). Também deve ser identificado em que parte(s) do sistema se encontram os perigos relevantes (reservatórios de pressão, armazéns, etc.). Para se proceder à identificação dos perigos existem diversos métodos e ferramentas, tais como:

- Checklists;
- PHA – "*Preliminary Hazard Analysis*", também conhecidas como HAZID – "*Hazard Identification*" ou RRR "*Rapid Risk Ranking*";
- FMEA – "*Failure Modes and Effects Analysis*";
- HAZOP – "*Hazard and Operability Analysis*";
- *Brainstorming*;
- Bases de dados (experiência).

Algumas questões devem ser consideradas quando se definem acontecimentos acidentais, nomeadamente:

- Que tipo de acontecimento é – Descreve o tipo de acontecimento (incêndio, fuga de gás, queda de objectos);
- Onde é que o acontecimento tem lugar – Descreve onde o acontecimento ocorre (na área de produção "A");
- Quando é que o acontecimento ocorre – Descreve as condições sob as quais o acontecimento ocorre (operação normal, arranque, durante a manutenção);
- A lista de acontecimentos acidentais que provêm do PHA, *brainstorming* ou outras metodologias de análise deve ser filtrada;
- Os acontecimentos acidentais diferentes são considerados para cada um dos elementos a ser analisado para saber onde estão os acontecimentos relevantes. Nesta relação pode-se usar uma matriz simples "acontecimento-elemento".

Os resultados desta etapa dão origem a uma listagem de todos os perigos significativos, uma listagem e descrição de todos os acontecimentos acidentais potenciais e relevantes e a identificação do local onde cada acontecimento acidental pode ocorrer. As causas de cada acontecimento acidental devem ser identificadas e descritas, fundamentalmente para identificar se as mesmas se prendem com factores técnicos, factores humanos, factores ambientais, factores sociais ou factores organizacionais. Os métodos e ferramentas usados na determinação das causas podem ser:

- FTA – "*Fault Tree Analysis*";
- BBN – "*Bayesian Belief Networks*" ("*influence diagrams*");
- Diagramas de causa-efeito (Ishikawa);
- RCA – "*Root Cause Analysis*";
- Bases de dados (*experience data*).

Como resultados, para cada acontecimento acidental potencial emergem:

- Todas as combinações de acontecimentos (falhas técnicas, erros humanos, cargas ambientais, etc.) que podem levar ao acontecimento acidental (*minimal cut set*);
- Os "*minimal cut sets*" podem ser usados para revelar fraquezas do sistema e criar uma base para melhorias.

Análise de Frequência – Após as causas do acontecimento acidental serem identificadas, estima-se a sua frequência (e como os acontecimentos acidentais podem ser evitados). Esta frequência pode ser estimada com base em:

- Bases de dados de incidentes anteriores;
- FTA (*Fault Tree Analysis*);
- Julgamento de especialistas (*expert judgement*).

Análise de Consequências – Com esta questão pretende-se identificar as consequências (imediatas e posteriores), dado o acontecimento acidental. Quando se analisam as consequências não nos devemos esquecer de toda a cadeia de acontecimentos resultante dos acontecimentos acidentais e as consequências imediatas, e as que não sendo aparentes, se revelam após algum tempo. É desejável classificar as consequências em diferentes categorias, como por exemplo:

- Pessoais (saúde e segurança);
- Ambientais;
- Económicas;
- Operacionais;
- Reputação da empresa.

Todas as cadeias de acontecimentos potenciais que se seguem a um acontecimento acidental devem ser identificadas e descritas. A maior parte dos sistemas têm uma ou mais funções de segurança (barreiras) que podem parar ou acabar com os efeitos do acontecimento acidental. A continuidade das cadeias dependerá do funcionamento, ou não, destas funções de segurança.

Avaliação do Risco – Na avaliação do risco deve-se averiguar com detalhe quais os riscos que estão presentes. O risco é uma função da frequência e das consequências dos acontecimentos acidentais. Muitas vezes, os acidentes podem ser representados graficamente de acordo com a frequência e severidade de um acontecimento. A Figura 3.2 mostra um exemplo dessa representação.

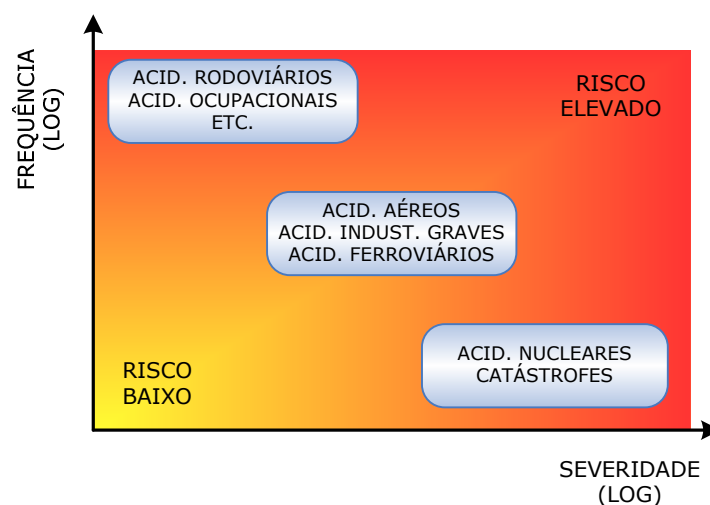



Figura 3.2 – Categorias de acidentes

[Fonte: Rausand & Hoyland (2004)]

Quanto maior for a frequência de ocorrência ou a severidade das consequências, então maior o risco. Uma ferramenta útil para descrever o risco é através de uma matriz. A Figura 3.3 ilustra um exemplo de uma matriz de risco.

FREQUÊNCIA / CONSEQUÊNCIA	1 POUCO	2 REMOTO	3 OCASIONAL	4 PROVÁVEL	5 FREQUENTE
4 CATASTRÓFICO					
3 CRÍTICO					
2 GRAVE					
1 MENOR					

	ACEITÁVEL, DE ACORDO COM O CRITÉRIO ESTABELECIDO
	ACEITÁVEL, SOB DETERMINADAS CONDIÇÕES
	NÃO ACEITÁVEL, NECESSÁRIO IMPLEMENTAR MEDIDAS DE REDUÇÃO DO RISCO

Figura 3.3 – Exemplo de uma matriz de classificação do risco

De referir que na execução de uma Análise de Modos de Falha e seus Efeitos (FMEA) também se deve incluir na construção das matrizes de risco um terceiro factor denominado "detectabilidade". Este factor permite distinguir entre os vários modos de falha aqueles que são muito facilmente detectáveis dos que são praticamente impossíveis de detectar. Para o efeito, e à semelhança dos outros dois factores, é também construída uma escala para a detectabilidade.

Aceitação do risco - Apesar de a aceitação do risco ser normalmente uma tarefa complicada e multifacetada, alguns princípios podem ser utilizados para determinar o que se pode entender por risco aceitável, como por exemplo:

- O princípio ALARP (*As Low as Reasonably Practicable*);
- Aceitação do risco, como definido na Norsok Z-013 (2001);
- O princípio MEM (*Minimum Endogeneous Mortality*);
- O princípio GAMAB (*Globalment Au Moins Aussi Bon*)

A Figura 3.4 descreve um dos princípios mais comuns em matéria de aceitação dos riscos; o princípio ALARP.

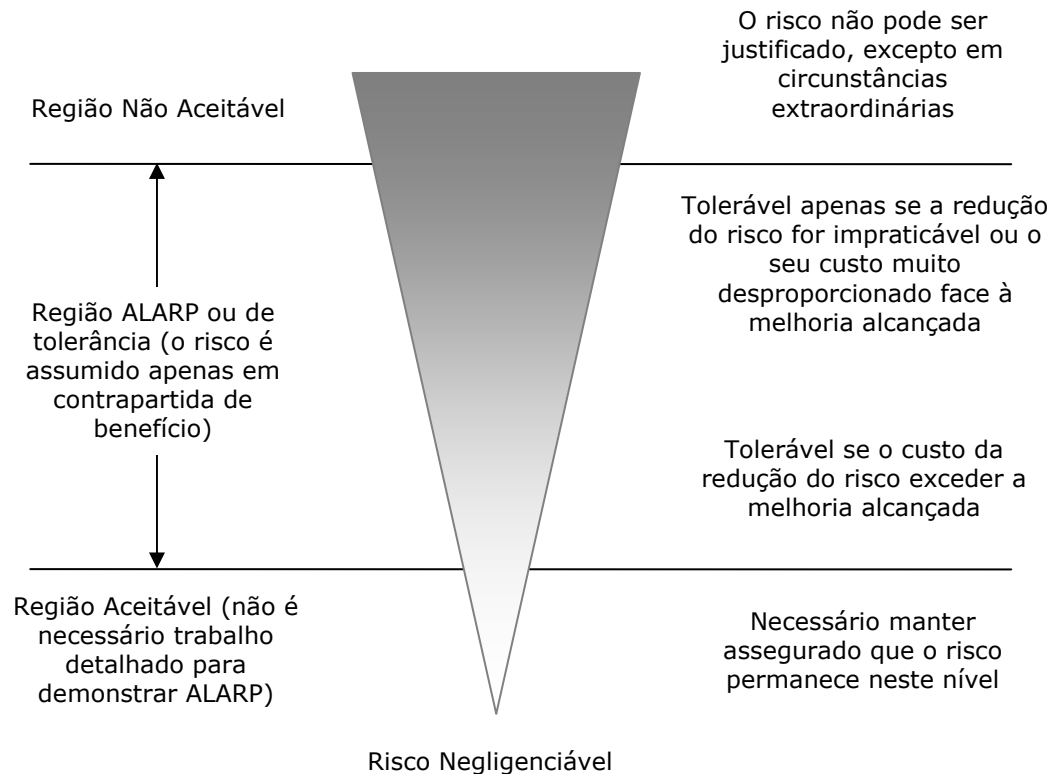



Figura 3.4 – Princípio de aceitação ALARP
[Fontes: NP EN 50126 (2000), Rausand & Hoyland (2004)]

3.2.2 – Gestão do Risco

Quando se fala de gestão de risco parte-se do pressuposto que essa mesma gestão é eficaz quando se conseguem manter os níveis de risco dentro de limites considerados aceitáveis. Na avaliação do risco verifica-se onde o mesmo se situa, podendo falar-se de risco insignificante, tolerável ou inaceitável. Quando se refere um risco tolerável há que efectuar sempre uma comparação entre os benefícios obtidos com a sua aceitação e os custos envolvidos na sua eventual redução. Outras comparações poderão ser efectuadas, dependendo do processo ou sistema em causa.

A gestão do risco engloba a análise do risco e complementa-a com a redução ou controlo desse risco através da tomada de decisões, implementação e monitorização de acções.

Quanto à eliminação do risco poder-se-ia dizer à partida que todos os factores de causa de acidentes (perigos) devem ser eliminados! No entanto, podem não existir os recursos para o fazer, pelo que se deve dar prioridade às acções correctivas, começando por as endereçar aos riscos mais elevados em detrimento dos riscos mais baixos.

Quando se efectuam análises de risco, deverão ser produzidos relatórios que reflectem essa análise. De acordo com a IEC 60300-3-9 (1995), o relatório deverá incluir:

1. Sumário e conclusões;
2. Objectivos e área de actuação;
3. Limitações, hipóteses e justificação de hipóteses;
4. Descrição dos subsistemas e componentes relevantes do sistema;
5. Metodologia de análise;
6. Resultados da identificação dos perigos;
7. Modelos usados, incluindo hipóteses e validação;
8. Informação e suas fontes;
9. Resultados do risco estimado;
10. Sensibilidade e análise de incertezas;
11. Discussão dos resultados (incluindo discussão das dificuldades analíticas);
12. Referências.

Por vezes surge algum criticismo sobre este tipo de abordagem, como por exemplo alguns comentários que referem que uma análise de risco consome muito tempo e recursos, ou que uma análise de risco é usada para abrandar processos de decisão, ou ainda que pode ser uma ferramenta manipulativa. Mas, em situações onde falta informação, as análises qualitativas, realizadas através do julgamento de especialistas é inevitável. A confiança nos resultados alcançados depende altamente da confiança nesses especialistas (qualificação e competência) e na eficácia dos procedimentos de análise. As incertezas serão reveladas e documentadas, em vez de escondidas. Quando devidamente realizada, uma análise de risco é muito transparente.

3.2.3 – Tratamento das Incertezas

Numa análise de risco, o factor probabilidade de ocorrência de um determinado evento reflecte um conjunto de incertezas que, através de uma abordagem menos cuidada poderá levar a conclusões completamente erradas e muito longe da realidade e da potencial ocorrência desse mesmo tipo de evento. Do mesmo modo, quando se fala nas

consequências, os cenários podem ser diversos, havendo também a incerteza associada à severidade ou gravidade do evento para cada cenário, caso ocorra.

As incertezas inerentes a uma análise de risco poderão ser quantificadas através da teoria da probabilidade, permitindo relacionar os diferentes tipos de variabilidade e as variáveis aleatórias entre si, sendo uma ferramenta excelente para tratar incertezas e quantificar o risco. Outras teorias alternativas têm sido desenvolvidas para tratar este tipo de problema, como por exemplo a teoria dos conjuntos vagos ou a teoria da possibilidade, mas não tão divulgadas ou experimentadas. Dentro da teoria da probabilidade duas escolas têm sido desenvolvidas, a escola frequentista e a escola bayesiana. Na frequentista, a probabilidade é quantificada como a frequência de ocorrência de determinado acontecimento, sendo bastante útil para caracterizar a variabilidade de um fenómeno que é representado por uma variável. Na bayesiana aceitam-se interpretações subjectivas das probabilidades, podendo as estimativas ser actualizadas de acordo com a disponibilidade de novas informações. A abordagem frequentista permite caracterizar fenómenos passados onde foram recolhidos dados e a bayesiana permite quantificar situações futuras, actualizando essas estimativas ao longo do tempo conforme se vão obtendo mais dados. Esta última é talvez a mais indicada para o tratamento das incertezas na análise e gestão de riscos.

A variabilidade de um fenómeno físico ou o grau de incerteza de acontecimentos futuros podem ser representados por variáveis aleatórias através de modelos físicos, matemáticos ou de outro tipo. Assim, existem dois tipos de incertezas, umas associadas às variáveis que são o resultado dos modelos utilizados, designadas por incerteza do modelo (ou epistemológicas) e as incertezas próprias de um dado fenómeno, designadas por variabilidade intrínseca natural ou aleatória.

Conforme descrevem Siu *et al* (1990), para cada área de aplicação específica, podem-se ter diversas fontes potenciais de incerteza. Como uma análise de risco serve de base para uma decisão, é importante que todas essas diferentes fontes de incerteza estejam explicitamente reflectidas nos resultados finais. Estes autores também descrevem dois tipos de incertezas.

- Incertezas da informação – incertezas referentes aos parâmetros usados num modelo particular. O seu impacto é determinado por rotina pela propagação das incertezas através do modelo (por exemplo através de simulações de Monte Carlo);

- Incertezas do modelo – incertezas associadas ao próprio modelo. Mesmo que se conheçam perfeitamente os parâmetros do modelo, obtêm-se imperfeições nos resultados do mesmo. Em situações onde os modelos usados fazem parte da análise de risco estas incertezas são conhecidas.

3.2.4 – Metodologias genéricas de análise de risco

A partir do que foi descrito nos parágrafos anteriores, e de acordo com Tixier *et al* (2002), foram identificadas mais de 60 metodologias de análise de risco (período de observação de 10 anos). Estas metodologias poderão incluir no seu desenvolvimento três fases principais (ou parte delas), nomeadamente:

- Fase de identificação, baseada na descrição do local;
- Fase de avaliação, para quantificação do risco (aproximação determinística e/ou aproximação probabilística) que nos transmite as consequências dos cenários e seus impactos;
- Fase de hierarquização dos resultados, que nos permite resolver os riscos mais importantes em primeiro lugar.

A primeira fase de identificação do risco é fundamental pois estabelece as bases da análise de risco. De facto, a informação da identificação do risco será a entrada para a avaliação e/ou hierarquização. Esta primeira fase deverá assim ser feita de forma exaustiva para se alcançarem os melhores resultados. A segunda fase, de avaliação, tal como mencionado anteriormente, deve ser realizada quer através da avaliação dos danos das consequências (determinística), quer pela avaliação da probabilidade de acidente (probabilística). A fase de hierarquização do risco coloca por ordem decrescente os riscos obtidos na fase anterior, de forma a implementar modificações ou acções correctivas nos sistemas de risco mais severo. Estas fases poderão não estar todas presentes. No entanto, em todas as metodologias será sempre necessário existir informação de entrada, informação de saída, e a descrição do método seleccionado.

As metodologias de análise de risco podem ser reunidas em dois grupos principais, nomeadamente:

- Metodologias Qualitativas;
- Metodologias Quantitativas.

Cada grupo pode ser dividido em três categorias:

- Determinístico;
- Probabilístico;
- Combinação de determinístico e probabilístico.

Os métodos determinísticos têm em consideração os produtos, o equipamento e a quantificação das consequências para vários alvos, como as pessoas, ambiente e equipamento. Os métodos probabilísticos são baseados na probabilidade ou frequência de situações perigosas ou na ocorrência de potenciais acidentes. Estes métodos focam principalmente a probabilidade de falha do equipamento ou dos seus componentes.

No estudo referido anteriormente (Tixier *et al*, 2002), a maior parte dos métodos são determinísticos. Tal aspecto deve-se ao facto de a maior parte dos analistas tentarem quantificar os danos e consequências de potenciais acidentes a partir da experiência anterior, antes de perceber o porquê e como eles podem ocorrer. A informação de entrada pode ser técnica ou qualitativa e pode ser dada através de planos ou diagramas, de processos e reacções, de substâncias, de probabilidades e frequências, de políticas e tipos de gestão, dados ambientais, de testes ou conhecimento histórico.

Os dados de saída podem ser tipo recomendações (qualitativos) ou indicar um índice relativo ao nível de risco (quantitativos). Ainda no referido estudo, propõem-se quatro classes de informação de saída, nomeadamente:

1) Tipo gestão (acções, recomendações, modificações e procedimentos de formação ou operação);
2) Tipo lista (listas de erros, efeito dominó, causas e consequências, modos de falha, cenários, etc.);
3) Tipo probabilístico (taxas de avarias, fiabilidade, probabilidade de cenários ou danos e frequência de acidente);
4) Tipo hierarquização (tipo índice de risco, severidade e criticidade, incêndio, explosão, índice organizacional e classificação conforme tipo de risco).

As Tabelas 3.1 e 3.2 mostram de uma forma resumida, respectivamente, os dados de entrada e dados de saída agrupados de acordo com os diferentes tipos de informação, conforme descrito no estudo referido anteriormente.

Tabela 3.1 – *Dados de entrada*

GRUPO	TIPO
Planos e Diagramas	Locais Instalações Unidades Redes de gás ou fluidos Funcionamento Barreiras de segurança Armazenagem
Processo e Reacções	Descrição das operações Descrição das tarefas Reacções e produções físicas e químicas Características dos processos Parâmetros cinéticos e calorímetros Condições de funcionamento normal Condições de operação
Produtos	Tipos de produto, propriedades físicas e químicas Quantidades Informação toxicológica
Probabilidade e Frequência	Tipo de falha Probabilidade de avaria Frequência de ignição e de avaria Erro humano Taxa de avarias Probabilidade de exposição
Política e Gestão	Manutenção Organização Política de segurança SMS Gestão de transportes Custo de equipamento
Ambiente	Ambiente local Informação topográfica Densidade populacional
Textos e conhecimento histórico	Normas Regulamentos e documentos Conhecimento histórico

Tabela 3.2 – *Dados de saída*

GRUPO	TIPO
Gestão	Acções Recomendações Modificações Procedimentos de formação e operação
Listagem	Lista de erros Estimativa / lista de riscos Lista dos efeitos de dominó Lista de causas/consequências da avaria Lista de actividades criticas Lista de modos de falha Lista de fontes de ignição Lista de locais vulneráveis Lista dos principais cenários
Probabilístico	Taxa de avarias Fiabilidade Probabilidade de cenários ou danos Frequência de acidentes
Hierarquização	Nível ou índice de risco Severidade ou criticidade Índice de incêndio ou explosão Índice de fugas tóxicas Índice de risco organizacional Classificação do tipo de risco

Para cada uma das metodologias apresentadas, são enunciados no referido artigo os respectivos campos de aplicação. A evolução das metodologias de análise de risco aponta que devam ser aplicados métodos simples, com um resultado final tipo índice de risco. A hierarquização (3ª fase) consiste em organizar a informação de uma forma crescente (ou decrescente). A maior parte das metodologias incluindo esta fase de hierarquização são geralmente quantitativas, e do tipo determinístico. São baseadas no desenvolvimento de um índice para o nível do risco, calculado para cada elemento, unidade ou área de uma forma escalonada.

Assim, são identificadas as áreas críticas de forma a realizar as acções prioritárias, diminuindo a probabilidade de ocorrência (prevenção) ou reduzindo as consequências de acidente (protecção).

Segundo Fernandez (1996), o desenvolvimento de um método de análise de risco probabilístico pode fornecer informação complementar à que é fornecida por uma análise determinística. Ainda de acordo com este autor, análises de risco de incêndio determinísticas e probabilísticas não são à partida consideradas concorrentes nem

aproximações mutuamente exclusivas. De acordo com Hostikka & Keski-Rahkonen (2003), os modelos determinísticos têm sido utilizados para estimar, por exemplo, as consequências de um incêndio, de acordo com uma série de variáveis de entrada. A incerteza da previsão depende de como as incertezas dos valores de entrada são transferidas para o sistema através do modelo.

Assim, surgem as barreiras de segurança que se destinam basicamente a prevenir a ocorrência de tais consequências de acontecimentos indesejáveis, ou, na sua eventualidade, diminuir ou mesmo mitigar os seus efeitos. No entanto, a condição de risco não se refere apenas à presença do perigo. A incerteza inerente à passagem do risco de potencial a actual ou real também é de ter em conta.

Devido à importância dos sistemas instrumentados de segurança (SIS) e dos sistemas de paragem de emergência (ESD) na diminuição do risco, Rouvroye & Blieck (2002) realizaram um estudo onde compararam várias técnicas de análise de segurança, classificando-as também em qualitativas e quantitativas. A Figura 3.5 mostra uma perspectiva dos autores sobre as técnicas mais usadas para esse propósito.

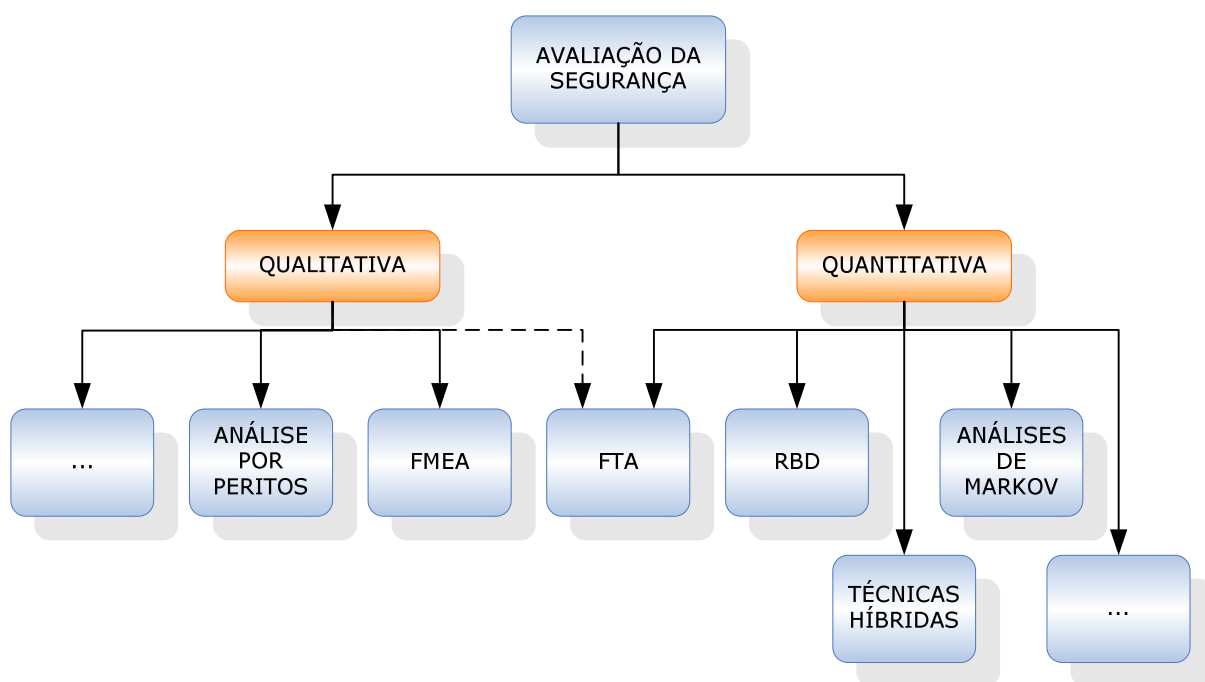



Figura 3.5 – Técnicas mais usadas para análise da segurança
[Fonte: Rouvroye & Blieck (2002)]

3.3 – Barreiras de Segurança

Desde o início dos tempos que as designadas barreiras de segurança têm sido instaladas com as mais diversas finalidades, fundamentalmente quando determinados tipos de risco estão presentes, servindo como uma medida de salvaguarda da vida humana, preservação ambiental ou para permitir a continuidade das actividades. O referido risco poderá estar relacionado com fenómenos naturais ou induzido pela humanização dos locais e industrialização dos processos.

Os conceitos de risco e de segurança encontram-se indubitavelmente ligados de uma forma pragmática e conceptual. O pragmatismo está subjacente, por exemplo, quando falamos da falta de segurança, medida pelo número de acontecimentos indesejados que ocorrem, e quando nos referimos ao aumento desse nível de segurança, também referimos à diminuição do nível de risco. Conceptualmente, é mais fácil ainda ligar os dois termos, bastando comparar as suas definições. Risco é, de uma forma simples, definido como a probabilidade de que algo indesejado possa acontecer. Segurança pode-se definir como a ausência desses acontecimentos indesejados (Hollnagel, 2008).

O projecto de sistemas de segurança é realizado tendo em conta uma disponibilidade específica para manter o risco dentro de limites considerados toleráveis. Se através de uma análise se verificar que o sistema possui uma disponibilidade abaixo do estipulado, efectuam-se alterações ao projecto inicial. Uma vez que as avarias dos sistemas de segurança podem, em muitos casos, resultar em morte, a abordagem a este tipo de equipamentos deverá ir no sentido de aumentar a sua disponibilidade, e por sua vez minimizar a ocorrência de potenciais mortes.

Os assuntos relativos ao projecto e operação de sistemas de segurança envolvem questões como o uso de redundâncias, diversidade de opções, selecção dos componentes, sistemas paralelos restritos em sensores e intervalos de tempo mais curtos entre testes e manutenções. A avaliação dos sistemas pode ser efectuada através de uma Análise de Árvore de Falhas em conjunto com uma metodologia de optimização, que pode incluir algoritmos genéticos (GA – *Genetic Algorithms*) ou outras técnicas (Andrews & Bartlett, 2005).

O conceito de barreira de segurança tem tido várias interpretações ao longo do tempo. Hollnagel (2004) afirma que "*enquanto as barreiras usadas para defender um castelo medieval eram na maior parte de natureza física, o princípio moderno de defesa em*

profundidade combina diferentes tipos de barreiras – desde a protecção contra a libertação de materiais radioactivos até ao relatório de acontecimentos e às políticas de segurança". Embora o conceito de defesa em profundidade tenha tido origem na indústria nuclear, o mesmo é empregue noutras áreas onde o risco é elevado.

Existem diversas normas e regulamentos onde a importância das barreiras de segurança é demonstrada tendo por base a redução do risco, tal como a IEC:61508 (1998), a IEC:61511 (2002), a Directiva Seveso II (1996) ou a Directiva Máquinas (1998), entre outras. No entanto, a própria definição de barreira de segurança é muitas vezes controversa de indústria para indústria, de sector para sector, ou de país para país, apresentando-se vários termos para idêntico significado, tais como barreiras, defesas, protecções, camadas, funções de segurança, etc… (Sklet, 2006).

Para se falar em barreira de segurança inevitavelmente teremos que referir o perigo que está subjacente, a fonte de energia responsável por esse perigo e uma sequência de acontecimentos. Normalmente, o termo barreira e função são empregues como sinónimos. No entanto, há que distinguir entre função de segurança e sistema de segurança quando nos referimos a barreiras. A primeira representa uma tarefa (e não um objecto) que corresponde ao impedimento da evolução do acidente de forma que o próximo acontecimento da cadeia nunca seja alcançado, enquanto um sistema pode consistir em um ou vários elementos, de diversos tipos, de maneira que a função da barreira seja alcançada (Svenson, 1991). Assim, a definição de barreira de segurança parece cobrir todas as fases da sequência do acidente, incluindo a prevenção, controlo e mitigação do mesmo.

Hollnagel (2008) define de uma forma clara a distinção entre as funções de segurança e os sistemas de segurança. A primeira descreve os modos através dos quais é genericamente possível prevenir ou proteger contra o transporte de massa, energia ou informação de uma forma descontrolada. A segunda refere-se aos meios pelos quais as funções das barreiras de segurança são realizadas. Ou seja, trata-se simplesmente de distinguir entre o que as barreiras *fazem* (funções) e o que as barreiras *são* (sistemas).

De acordo com um estudo muito completo sobre este tema (Sklet, 2006), "***as barreiras de segurança são meios físicos e/ou não físicos planeados para prevenir, controlar ou mitigar acontecimentos indesejáveis ou acidentes***". Planeado significa que pelo menos um dos meios referidos tem como objectivo a redução do risco. Prevenir significa reduzir a probabilidade do acontecimento perigoso, controlar tem a ver

com a limitação da extensão ou duração desse acontecimento, enquanto mitigar é reduzir os seus efeitos. Acontecimentos indesejáveis são todos os que se referem a avarias técnicas, erros humanos, acontecimentos externos ou uma combinação destes que possa conduzir a potenciais perigos, enquanto acidentes se refere a acontecimentos não desejados ou não planeados que levam a danos humanos, ambientais ou em equipamento.

Se a função é realizada com sucesso, isto significa que se obtem um efeito significativo na ocorrência e/ou nas consequências. Uma função deve ser descrita através de um verbo e de um substantivo, como por exemplo "*parar motor*" ou "*fechar válvula*". No projecto ARAMIS (*Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive*) são sugeridos os verbos "*evitar*", "*prevenir*", "*controlar*" e "*proteger*" para definir genericamente as funções das barreiras. A Figura 3.6 representa, de uma forma geral, as funções de uma barreira de segurança.

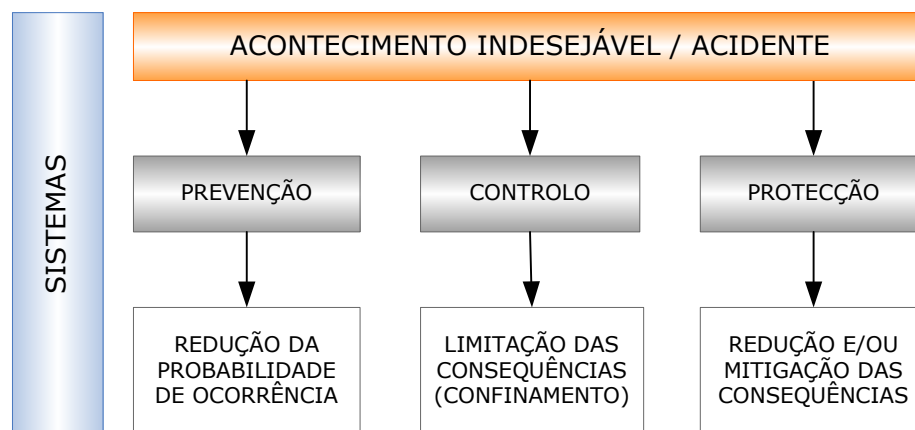



Figura 3.6 – Funções das barreiras de segurança

Sklet (2006) ainda define um sistema tipo barreira como "***um sistema que foi projectado e implementado para realizar uma ou mais funções da barreira de segurança***". Se o sistema funciona, a função é cumprida.

De salientar que um sistema tipo barreira pode ter várias funções e que em alguns casos vários sistemas são necessários para cumprir uma única função. Por definição, um elemento do sistema é um componente (ou subsistema) que por si só não é suficiente para cumprir a função da barreira. Um sistema tipo barreira de segurança poderá ter vários tipos de elementos (elementos físicos, actividades executadas por pessoas, ou uma combinação destes).

No fundo, questões como a redução da probabilidade de ocorrência, redução das consequências ou prevenção do fluxo reduzem-se a definir funções das barreiras de segurança. No conceito de barreiras de segurança duas perspectivas ou modelos podem surgir: O modelo de energia e o modelo de processo. No primeiro, o princípio básico é o de separar os perigos das vítimas, enquanto no segundo modelo se trata de separar o acidente em diferentes fases, ajudando a entender como o sistema se degrada gradualmente desde o estado normal até ao momento de acidente.

De referir que quando se refere vítima, se está a identificar o potencial receptor das consequências emanadas pela fonte de energia, quando o acontecimento indesejável ocorre. De seguida apresentam-se algumas definições sobre a classificação das funções e classificação dos sistemas, assim como considerações acerca do desempenho das barreiras de segurança.

3.3.1 - Classificação das funções das barreiras de segurança

As barreiras de segurança possuem apenas duas funções principais; prevenção e protecção (Hollnagel, 2004). As barreiras de segurança descritas como meio de prevenção são aquelas onde se pretende uma actuação antes do início de um acontecimento específico, tendo por função assegurar que esse acontecimento não ocorra ou que pelo menos abrande o seu desenvolvimento. As barreiras de segurança que actuam depois do início do acontecimento ter ocorrido, e que supostamente protegem as pessoas, o ambiente e/ou os equipamentos das consequências do acidente, correspondem a meios de protecção. Nesta classificação, a protecção engloba o controlo e a mitigação, embora também muitas vezes se possa dizer que o controlo faz parte da prevenção, dependendo esta classificação da definição que se utilizar para o acontecimento inicial.

Como na prática é impossível prevenir completamente a ocorrência de acontecimentos considerados indesejados, ou seja, eliminar o risco por completo numa perspectiva de eliminação da probabilidade de ocorrência de acidentes (ou incidentes indesejáveis), a melhor forma de assegurar a máxima segurança é conciliar estas duas aproximações, conjugando a prevenção com a protecção e usar as barreiras de segurança para o efeito. Um sistema seguro é aquele onde nada de indesejado ocorre, quer seja na prevenção de acontecimentos indesejados, quer na protecção de consequências indesejadas.

Normalmente a actuação de um sistema de protecção pressupõe colocar o processo (produtivo, ou não) numa situação de paragem parcial ou eventualmente paragem total, o que é aceitável uma vez que o objectivo muitas vezes não é promover a continuidade das actividades a todo o custo, mas sim a segurança de sistemas mais abrangentes, como a salvaguarda de um conjunto de pessoas ou protecção do ambiente (como em casos de acidente em centrais nucleares).

Para actuar ao nível da prevenção e da protecção é necessário inicialmente conhecer o(s) risco(s) que podem estar presentes. A forma para alcançar este objectivo passa por realizar análises de risco, tal como referenciado em parágrafos anteriores neste capítulo. Para descrever um acontecimento crítico pode-se assim olhar para as suas causas e para as suas consequências, podendo esta abordagem ser graficamente representada através do designado modelo tipo laço (*bow-tie*) (Delvosalle *et al*, 2005), conforme Figura 3.7.

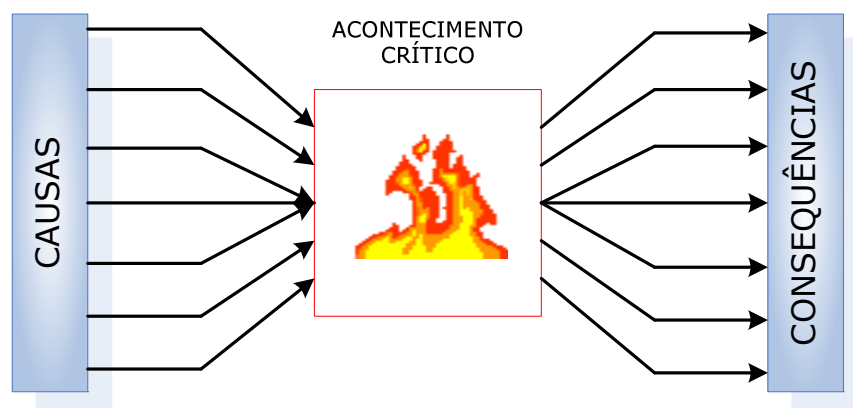



Figura 3.7 – Modelo tipo laço

No lado esquerdo do laço (causas) podem-se utilizar metodologias como Análises de Árvore de Falhas (FTA = *Fault Tree Analysis*), Diagramas de Blocos de Fiabilidade (RBD = *Reliability Block Diagrams*), Análises de Modos de Falha e Efeitos (FMEA = *Failure Modes and Effect Analysis*) ou bases de dados. Quanto ao lado direito do diagrama (consequências) podem ser utilizadas outras ferramentas como Análises de Árvore de Acontecimentos (ETA = *Event Tree Analysis*), modelos de consequência ou simulação.

Dianous & Féviez (2006) afirmam que para barreiras do tipo "prevenir" ou "controlar" se pode aplicar uma regra que relaciona o nível de confiança[8] da barreira - LC (*Confidence Level*) com a frequência do acontecimento crítico poder ocorrer, onde para um determinado LC da barreira, a sua probabilidade de ocorrência é reduzida de um factor 10^{-LC} (ver exemplo da Figura 3.8).

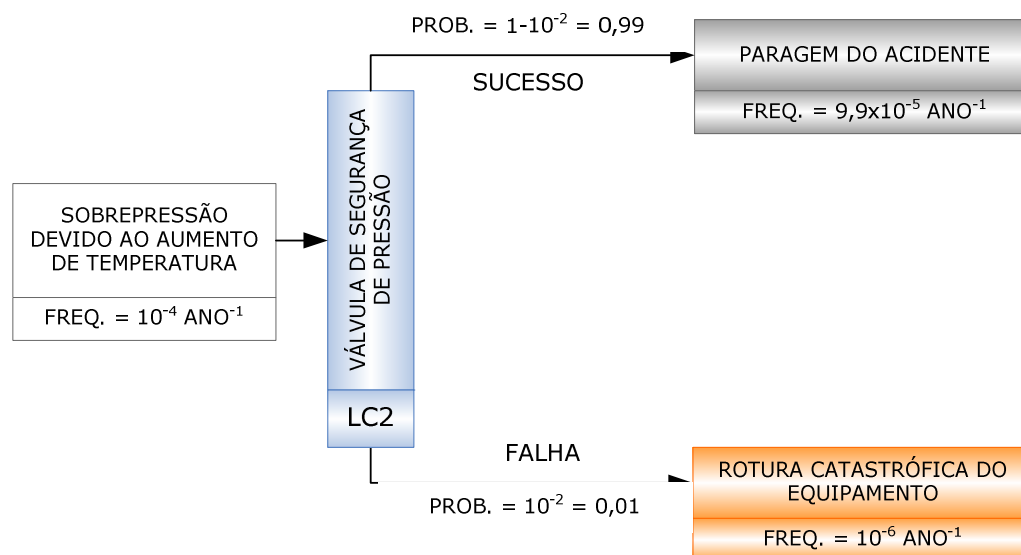



Figura 3.8 – Barreiras de segurança tipo prevenir ou controlar

Por fim, dado que o acontecimento potencialmente perigoso ocorre, é necessário proteger os alvos vulneráveis das consequências desse mesmo acontecimento. Estaremos agora do lado direito do modelo tipo laço da Figura 3.7, onde se analisa a influência do desempenho da barreira de segurança nos efeitos de fenómenos perigosos, quer a barreira tenha sucesso ou falhe.

Outro ponto de vista relacionado com a classificação das barreiras de segurança distingue entre funções de segurança criticas primárias, secundárias e terciárias, correspondendo a sistemas técnicos físicos, a actividades realizadas para manter as funções primárias e sistemas de gestão, respectivamente. Similarmente a esta classificação aparecem outros estudos, onde estas mesmas designações apresentam descrições com pequenas adaptações (Sklet, 2006).

---

[8] LC, ou nível de confiança, é um valor ligado à fiabilidade da barreira de segurança, sendo inversamente proporcional à probabilidade de falha quando solicitado. Para o nível de confiança da barreira assume-se um valor idêntico ao SIL – *Safety Integrity Level*, descrito mais à frente no presente capítulo.

3.3.2 - Classificação dos sistemas de segurança

Normalmente os sistemas de segurança são distinguidos em dois tipos fundamentais: barreiras físicas e barreiras não físicas, ou eventualmente num terceiro tipo resultante da combinação dos dois tipos anteriores. Outro tipo de classificação é apresentado (Sklet, 2006), diferenciando entre barreiras físicas, técnicas e administrativas, em que as primeiras se referem a sistemas concebidos no projecto de construção, as barreiras técnicas são sistemas que actuam quando o perigo se torna eminente e por fim as barreiras administrativas, que caracterizam procedimentos e sistemas inseridos numa lógica de gestão. Outras abordagens relativas à classificação dos sistemas de segurança poderão ser encontradas, como designações relativas a barreiras de carácter organizacional, ou barreiras relacionadas com factores humanos (Svenson, 1991) (Neogy *et al*, 1996) (Kecklund *et al*, 1996).

De acordo com a norma IEC:61511 (2002), as medidas de redução do risco encontram-se definidas para:

- Sistemas instrumentados de segurança (SIS);
- Sistemas relacionados com a segurança com outra tecnologia, que não SIS;
- Serviços para redução do risco externo.

Um sistema instrumentado de segurança refere-se a qualquer combinação entre sensor(es), unidade(s) de tratamento lógico e elemento(s) final(is). Outros sistemas de segurança poderão utilizar tecnologias que não a eléctrica, electrónica ou electrónica programável, tal como definido em (IEC:61508, 1998), como por exemplo uma válvula de alívio de pressão ou um sistema automático de extinção de incêndio. Por fim, classificam-se determinados serviços que promovem a redução do risco oriundo do exterior, independentemente do tipo de tecnologia utilizado (por exemplo uma parede corta fogo, normalmente designada por *firewall*).

No que se refere à classificação de sistemas de segurança, também é comum surgir a distinção entre sistemas activos e sistemas passivos. Enquanto os sistemas passivos se encontram inseridos no projecto da instalação e são independentes do sistema de controlo operacional, os sistemas activos dependem de acções humanas ou sistemas de controlo técnico para actuar (Kjellén, 2000). Nos sistemas activos de protecção existe uma transição de um estado para outro como resposta a uma alteração de uma ou mais

propriedades (por exemplo alteração da temperatura de um reservatório) ou devido a um sinal enviado por outro elemento (por exemplo o accionamento de um interruptor de alarme manual). Assim, um sistema activo pressupõe a existência de um qualquer sensor, de um processo de decisão e de uma acção.

Sklet (2006) refere um trabalho onde se tipificam dois tipos de sistemas de segurança: Sistemas inerentes e sistemas adicionais, correspondendo os primeiros a barreiras criadas através da alteração de um parâmetro de projecto (por exemplo aumentando a espessura da parede de um reservatório) e os segundos referindo-se à introdução de sistemas ou componentes introduzidos especificamente devido a questões de segurança (por exemplo um sistema automático de extinção de incêndio – *sprinklers*).

Pode-se também distinguir entre barreiras permanentes ou *on-line* e barreiras activadas, temporárias ou *off-line* (Hollnagel, 2004), consoante as mesmas funcionem permanentemente ou apenas quando ocorrer uma sequência de acções (detecção, diagnóstico e acção) ou durante um determinado período de tempo. Hollnagel (2008) afirma ser suficiente caracterizar os sistemas das barreiras de segurança em quatro tipos:

- Físicas ou materiais;
- Funcionais;
- Simbólicas;
- Incorpóreas.

Físicas ou materiais – Na prevenção de um acontecimento ou na mitigação dos efeitos, impedindo o transporte de massa, energia ou informação de um local para outro. São exemplos de barreiras físicas os edifícios, paredes, portões, cortinas corta-fogo, etc. Este tipo de barreiras de segurança possuem a característica de não ser necessário haver um reconhecimento ou interpretação por alguém para funcionar.

Funcionais – Necessitam de uma ou mais pré-condições para actuar. Algumas barreiras funcionais necessitam que alguém actue para lhe alterar o estado, enquanto outras são autónomas dependendo de condições externas.

Simbólicas – Necessitam da interpretação de alguém. É o caso de sinais visuais ou sonoros, avisos e alarmes, entre outros.

Incorpóreas – Não se encontram fisicamente presentes, dependendo do conhecimento das pessoas. Na indústria, este sistema de barreiras é sinónimo de barreiras organizacionais, como por exemplo regras, leis ou restrições impostas pela organização, independentemente de serem físicas, funcionais ou simbólicas.

3.3.3 - Desempenho das barreiras de segurança

Embora para cada caso específico se possa classificar a barreira de segurança de acordo com as várias funções e tipos de sistemas anteriormente referidos, torna-se fundamental analisar o desempenho das mesmas. Os critérios usados para avaliar o desempenho das barreiras de segurança dependem de cada aplicação, podendo-se, de uma forma geral, efectuar uma análise em três fases distintas:

- Durante e após testes ou ensaios;
- Durante e após a ocorrência de acidentes ou situações indesejáveis;
- Durante análises de risco, na avaliação dos vários cenários possíveis.

A análise do desempenho, independentemente da situação em que ocorra, serve para perceber quais as barreiras que existiam e como estas se comportaram, quais as que não foram usadas e aquelas que não existindo se tornavam necessárias. De acordo com a *Petroleum Safety Authority* (2002) o desempenho das barreiras de segurança pode ser avaliado através dos seguintes critérios:

- Funcionalidade/Eficiência - Efeito da barreira na sequência do acontecimento se esta cumpriu a sua função;
- Disponibilidade/Fiabilidade - Capacidade de funcionar quando solicitado;
- Robustez - Capacidade de funcionar durante a sequência do acidente ou mesmo sob influência deste.

Conforme descrito por Neogy *et al* (1996), o termo fiabilidade e eficácia relatam o sucesso das barreiras de segurança em matéria de protecção. A fiabilidade relaciona-se com a capacidade de resistir a avarias, enquanto a eficácia de uma barreira demonstra como essa mesma barreira se comporta na protecção do perigo específico. De acordo com a Tabela 3.3, que reflecte um estudo feito por Hollnagel (2004), são apresentados alguns requisitos para as barreiras de segurança.

Tabela 3.3 – *Requisitos para as barreiras de segurança*

Critério	**Requisito específico**
Adequação	Capaz de prevenir todos os acidentes dentro do projecto Cumprir os requisitos legais (normas, regulamentos) Não deve exceder as capacidades do sistema primário Se uma barreira é inadequada, deverão ser criadas barreiras adicionais
Disponibilidade/Fiabilidade	Quando a barreira é activada, todos os sinais devem ser detectáveis As barreiras activas devem identificar avarias seguras, possuir auto-teste ou ser testadas regularmente As barreiras passivas devem ter uma rotina de inspecção
Robustez	Capaz de suportar acontecim. extremos (incêndio, inundação, …) A barreira não deve ser desactivada com a entrada de outras Barreiras Duas barreiras não devem ser afectadas pela mesma causa comum
Especificidade	Os efeitos da activação da barreira não devem conduzir a outros acidentes A barreira não deve destruir aquilo que ela própria protege

Já outros trabalhos (Dianous & Fiévez, 2006) mostram que a avaliação de barreiras de segurança é realizada de acordo com três critérios, que servirão para encontrar uma determinada redução do risco, nomeadamente:

- Eficácia;
- Tempo de resposta;
- Nível de confiança.

Sendo a eficácia de uma barreira de segurança a sua capacidade para cumprir a função de segurança durante um determinado tempo, em condições específicas, sem apresentar modos de degradação. Esta eficácia pode ser representada por uma probabilidade do desempenho da função de segurança, que pode variar durante o tempo em que o sistema de segurança actua. O tempo de resposta corresponde à duração de tempo que medeia entre o momento em que a barreira é solicitada até se atingir por completo a função de segurança.

O nível de confiança de uma barreira de segurança está ligado à fiabilidade, e desta forma também se pode representar por uma probabilidade, correspondente neste caso à probabilidade de falha quando solicitada (PFOD – *Probability of Failure On Demand*) e cumprindo a função requerida, durante o intervalo de tempo estabelecido e para uma eficácia pré-definida. O nível de confiança de uma barreira de segurança é inversamente proporcional à PFOD. Este conceito é idêntico à noção de Nível de Integridade de Segurança (SIL = *Safety Integrity Level*) definido para os sistemas instrumentados de segurança (SIS = *Safety Instrumented Systems*) na IEC:61511 (2002), que num

contexto operacional também é influenciado pelo sistema de gestão da segurança que estiver presente.

Num estudo (Hollnagel, 2008) efectuado para vários critérios de avaliação do desempenho das barreiras de segurança, é apresentada uma comparação entre os vários tipos de sistemas, tendo em conta a sua qualidade e apresentando algumas vantagens e desvantagens. Aqui, pode ser visto que as barreiras físicas são aquelas que apresentam valores mais elevados na avaliação dos critérios, apresentando no entanto desvantagens em termos de custos e tempo dispendido para a sua implementação, assim como na maior parte dos casos necessitarem de intervenções de manutenção com determinada frequência.

Para certos tipos de barreiras de segurança, a sua manutibilidade também deverá ser ponderada como critério de avaliação do seu desempenho, uma vez que a facilidade com que as intervenções de manutenção podem ser realizadas também pode levar a maiores ou menores tempos para repor o seu estado operacional em caso de avaria, e consequentemente variando a sua disponibilidade. Também deve ser tida em conta a dificuldade que muitas vezes ocorre em diagnosticar as referidas barreiras de segurança.

Os requisitos funcionais de uma barreira de segurança podem estar explícitos em regulamentos, normas, códigos de projecto, etc., ou em requisitos baseados em análises de risco com o respectivo critério de aceitação definido. A fiabilidade e disponibilidade de uma barreira de segurança correspondem aos SIL exigidos pela IEC:61511 (2002), sendo o seu nível de confiança determinado como descrito no projecto ARAMIS, já citado anteriormente. Os requisitos SIL, referentes à análise funcional de sistemas, constantes na IEC:61508 (1998) e na IEC:61511 (2002) encontram-se descritos na Tabela 3.4.

Tabela 3.4 – *Níveis de Integridade de Segurança (IEC:61511)*

Nível de Integridade de Segurança (SIL)	Modo – Baixa Solicitação PFOD média	Factor de Redução do Risco	Modo – Op. Contínua Frequência de avarias perigosas para realizar a função [h^{-1}]
4	$\geq 10^{-5}$ a $<10^{-4}$	100000 a 10000	$\geq 10^{-9}$ a $<10^{-8}$
3	$\geq 10^{-4}$ a $<10^{-3}$	10000 a 1000	$\geq 10^{-8}$ a $<10^{-7}$
2	$\geq 10^{-3}$ a $<10^{-2}$	1000 a 100	$\geq 10^{-7}$ a $<10^{-6}$
1	$\geq 10^{-2}$ a $<10^{-1}$	100 a 10	$\geq 10^{-6}$ a $<10^{-5}$

Os dois modos de solicitação indicados na Tabela 3.4 referem-se a:

- PFOD média ou baixa solicitação – Quando a frequência de solicitação para o sistema operar não é superior a duas vezes a frequência de teste ou ensaio;
- Alta solicitação ou modo contínuo de operação – Probabilidade de ocorrer uma avaria perigosa por hora, sendo utilizada quando a frequência de solicitação do sistema para actuar é superior a duas vezes a frequência de teste ou ensaio, ou quando o mesmo opera em modo contínuo.

A IEC:61508 – Parte 4 (1998) refere um intervalo arbitrário de um ano para distinguir os dois modos de solicitação. Os mesmos aparentam, à primeira vista, ter universos diferentes quanto às unidades, pois enquanto no modo de baixa solicitação a referência é a um ano (por definição), no funcionamento contínuo refere-se a avarias perigosas por hora. No entanto, se for considerado o facto de existirem perto de 10000 horas por ano (cerca de 8760 horas), os dois modos têm aproximadamente as mesmas métricas de segurança.

Antes de se efectuar uma estimativa quantitativa do nível de confiança devem ser estudados alguns parâmetros qualitativos, tais como (Dianous & Fiévez, 2006):

- A independência da barreira de segurança relativamente às causas e sistemas de regulação para reduzir as avarias tipo causa comum (CCF = *Common Cause Failures*);
- A arquitectura do sistema de segurança, para verificar a existência de redundâncias, modos de falha de causa comum, se as barreiras têm avarias seguras, etc…;
- O conceito de "testado" relativamente à barreira, sustentado em experiências anteriores;
- A existência de testes periódicos, de acordo com as instruções dos especialistas, fornecedores ou fabricantes, assim como a existência de um programa de manutenção.

Relativamente ao cálculo do nível de confiança das barreiras de segurança, e quanto a constrangimentos arquitecturais, utilizam-se dois parâmetros:

- A função de avaria segura (SFF = *Safe Failure Function*), que traduz o quociente entre a frequência de avaria do componente que conduz a uma posição segura (que potencialmente não coloca a barreira num estado de falha funcional) e a frequência total das avarias;

- A tolerância à falha, ligada à capacidade da barreira se manter funcional em termos de segurança em caso de avaria de um ou mais sistemas que a compõem. Este aspecto está ligado à existência de redundâncias.

No aspecto quantitativo, a estimativa do nível de confiança processa-se de uma forma semelhante, mas agora tendo em conta o modo de solicitação, tal como definido na Tabela 3.4, onde o valor do nível de confiança da barreira corresponde ao nível de Integridade de Segurança (SIL).

Para a determinação do valor global do nível de confiança de uma barreira de segurança, têm-se em conta os aspectos qualitativos e os aspectos quantitativos dos diversos subsistemas que constituem essa barreira. O valor global corresponderá ao menor dos valores encontrados para os subsistemas considerados. De acordo com Dianous e Fiévez (2006), no sector industrial, é muito difícil encontrar níveis de confiança tipo LC 4. Conforme a Tabela 3.4 também mostra, a cada nível de confiança corresponde um factor de redução do risco.

Outro conceito relacionado com uma forma simplificada de análise quantitativa do risco denomina-se Análise da Camada de Protecção (LOPA = *Layer Of Protection Analysis*). Gowland (2006), no seu trabalho, compara esta metodologia com uma figura de uma cebola, onde as barreiras de protecção são constituídas por sistemas de segurança que se encontram:

- No próprio projecto;
- Nos parâmetros de segurança utilizados;
- No controlo do próprio processo e na capacidade de desligar o processo de forma segura;
- Em equipamentos mecânicos;
- Em barreiras físicas e organizacionais.

Quando estas barreiras não forem suficientes para evitar a ocorrência do acidente devem ser adicionadas mais camadas através de sistemas instrumentados de segurança. A frequência do acidente perigoso que se estiver a estudar é considerada, e o objectivo estabelecido como entrada na região aceitável para essa ocorrência denomina-se o objectivo (ou alvo) LOPA. Quando este valor, considerado aceitável, é estipulado por norma ou por entidades reguladoras, tudo se torna mais fácil uma vez que assim se evita que cada instalação estabeleça os seus próprios critérios. A Figura 3.9 mostra o princípio de funcionamento das várias camadas ou barreiras (independentes) e a sua influência

em termos de frequência das consequências finais de acordo com a PFOD de cada barreira e partindo de uma frequência estimada para o acontecimento inicial.

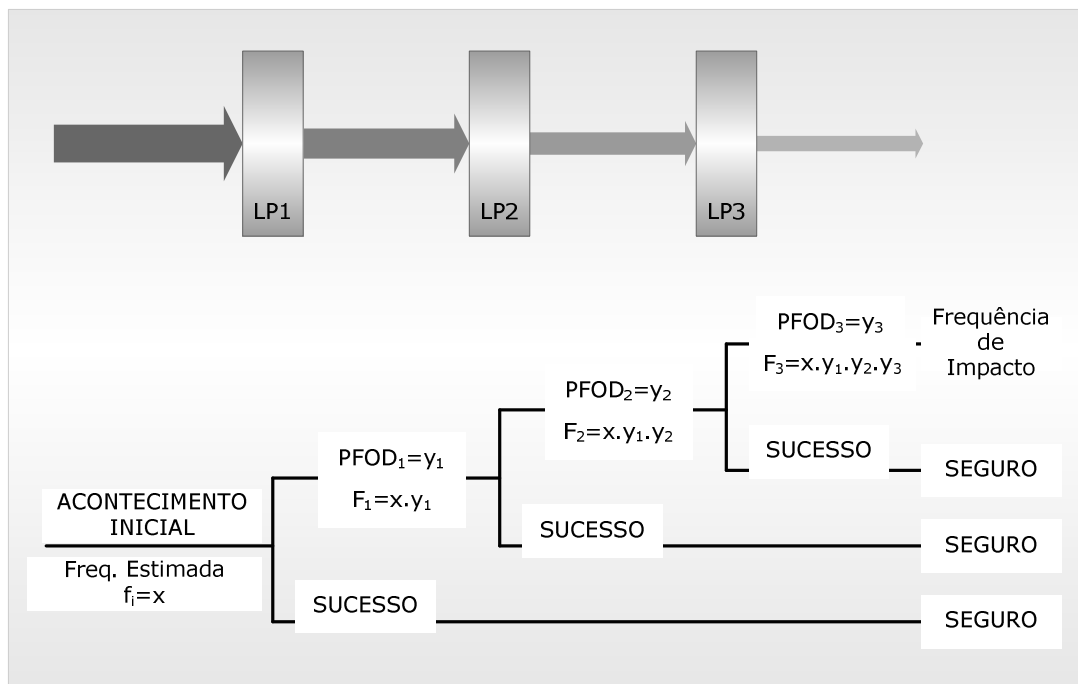



Figura 3.9 – Conceito LOPA

De acordo com Gowland (2006) as dificuldades encontradas na avaliação do desempenho das barreiras de segurança prendem-se em alguns casos com a análise do valor de mitigação das barreiras e o verdadeiro efeito de barreiras processuais, tais como sistemas de inspecção ou gestão.

Ao se efectuar uma análise total às barreiras de segurança terão que ser tidos em conta todos os aspectos, incluindo alguns efeitos adversos que a implementação dessas barreiras de segurança pode acarretar, tais como os inerentes custos acrescidos, a necessidade de intervenção para manutenção e por vezes a introdução de novos perigos.

Quando se está a tratar o projecto e instalação de barreiras de segurança é necessário que se conheçam à priori os riscos potenciais. Estes riscos podem ser avaliados como ameaças expectáveis e conhecidas face aos elementos específicos da instalação ou organização e tendo por base experiências anteriores, ou, por outro lado, ameaças cujo desenvolvimento é imprevisível, tornando mais difícil estipular o tipo de barreira de protecção. De qualquer forma, é sempre necessário pensar no futuro, para que numa perspectiva de prevenção ou protecção se diminua o risco. O desempenho de uma

barreira de segurança depende de como a mesma é projectada, utilizada durante a operação e inspeccionada e mantida durante o seu ciclo de vida (Duijm, 2008).

Reconhece-se um conjunto de factores de gestão, importantes para assegurar o desempenho de uma barreira de segurança. Por exemplo, as barreiras físicas dependem fundamentalmente de factores como a identificação do risco, o projecto, a instalação, a gestão de sobressalentes, inspecção e manutenção, enquanto as barreiras sustentadas na acção humana dependem mais dos procedimentos, planeamento, treino, empenho, coordenação e comunicação. Duijm & Goossens (2006) apresentam no seu estudo uma forma de quantificação das acções de gestão no desempenho das barreiras de segurança, baseada na combinação de pesos e pontuações.

3.4 – Risco de Incêndio

Conforme se viu anteriormente, o risco estará sempre presente, pelo que tentar-se-á optar pela solução que apresente um risco menor face aos objectivos a alcançar, havendo lugar assim à aceitação de um determinado nível de risco. A metodologia para resolver estes problemas é habitualmente genérica mas, no entanto, há que ter em atenção certos pormenores conforme a natureza e dimensão da população envolvida nos riscos analisados.

Quando se fala em risco para uma dada instalação, de uma forma geral, pode-se estar a transmitir este conceito de uma forma muito globalizada, perdendo-se por vezes a noção de quais os riscos específicos que estão em jogo e a sua contribuição ou influência para uma ideia ou valor final encontrado. Assim, convém realçar cada risco particular, focalizando o trabalho naquele cuja incerteza associada poderá revelar resultados mais negativos para os objectivos definidos.

Para determinada empresa, por exemplo, devido à sua localização geográfica pode-se pretender efectuar uma análise de risco sísmico, enquanto para outra, por motivos da sua baixa tecnologia e elevada utilização de operações manuais se poderá analisar o risco de acidentes de trabalho, ou ainda outro caso onde devido ao elevado valor de emissões para a atmosfera se queira saber o risco ambiental para uma determinada região.

No caso específico do presente trabalho, e devido à crescente preocupação de vários sectores da indústria a nível nacional e mundial, pretende-se analisar o **risco de**

incêndio em instalações industriais, uma vez que na maior parte dos casos um acontecimento desta natureza pode ter consequências catastróficas, pondo em causa vidas humanas, equipamentos, a continuidade das actividades desenvolvidas ou causando danos ambientais.

Tratando-se de instalações industriais de risco elevado, fortalece-se a importância desta análise, pelo que a abordagem passa primeiramente por verificar as medidas de prevenção estabelecidas e os meios de protecção contra incêndios existentes, assim como a conformidade da instalação com a legislação quanto a estes requisitos.

De acordo com Johansson (2001), os investimentos relacionados com a segurança contra incêndios não costumam ser vistos como uma fonte de receita mas sim como decisões associadas a despesas, não só de investimento, como também de manutenção. No entanto, esses investimentos poderão, por exemplo, significar uma redução no prémio de seguro, o que por si só já poderá ser encarado como uma receita.

Outra questão bastante importante é saber como avaliar a redução do risco de incêndio que o investimento envolve, cuja missão ou tarefa não é fácil, uma vez que a ocorrência e propagação de um incêndio são altamente incertas, não se sabendo quantos incêndios irão ocorrer durante o prazo do investimento, ou qual a extensão dos mesmos, caso ocorram.

O risco de incêndio na indústria é uma das principais preocupações de qualquer gestor ou responsável pela gestão do risco numa organização, tornando-se em certos casos o factor primordial para garantir a continuidade das actividades, por vezes fulcrais para um determinado sector económico ou até mesmo para o próprio país. A importância desta preocupação pode ser expressa pelas avultadas verbas que normalmente são exigidas pelas seguradoras aos seus clientes para cobertura desse tipo de risco.

Existem diversas ferramentas e métodos de abordagem a esta questão, tendo-se optado por desenvolver no presente trabalho uma nova metodologia, que embora não analise o risco no seu todo, poderá ser um contributo quando tal for o objectivo dos estudos realizados. Pretende-se que esta metodologia transmita o rigor e a coerência científica exigida, mas que ao mesmo tempo tenha aplicabilidade no contexto industrial.

3.4.1 – Factores a considerar no risco de incêndio

A descoberta do fogo permitiu ao Homem dar um salto no progresso da civilização, sendo porventura uma das maiores descobertas da Humanidade. Infelizmente, quando não se consegue controlar essa fonte de energia, ocorre um incêndio, deixando o fogo de ser encarado como um bem fundamental e passando a transformar-se numa preocupação, por vezes fatal para a vida humana e catastrófica para a sociedade.

Um incêndio é o resultado de uma combustão (ou várias), fazendo necessariamente parte da(s) mesma(s) três componentes: os materiais combustíveis, o comburente (oxigénio) e a energia de activação. Esta simultaneidade de factores nas devidas proporções e de forma não controlada pode transformar-se numa tragédia.

Assim, a prevenção e o combate aos incêndios passa pela separação ou controlo destes factores, ou pela eliminação de algum deles. O objectivo principal da segurança contra incêndios é a salvaguarda das vidas humanas. Além deste objectivo outros poderão surgir, nomeadamente:

- Facilitar a intervenção dos meios de socorro exteriores;
- Proteger os bens materiais, com prioridade para as edificações vizinhas;
- Promover a continuidade das actividades.

De uma forma geral, e de acordo com a teoria clássica, o risco de incêndio potencialmente presente em determinada instalação pode ser apresentado como o produto de dois factores; a probabilidade de ocorrência do incêndio e a gravidade (ou consequências) relacionadas com tal acontecimento.

Pode-se então diminuir ou limitar o risco através da adopção de medidas que permitam reduzir qualquer um destes factores, elevando o nível de segurança. Ao reduzirmos a probabilidade de ocorrência de incêndio estamos a actuar na **“prevenção”**, enquanto ao procurarmos reduzir os efeitos da sua gravidade estamos no âmbito da **“protecção”**.

Enquanto o primeiro se relaciona fundamentalmente com o tipo e quantidade de combustível e com as fontes de ignição presentes na instalação, o segundo factor tem a ver em grande escala com as medidas de protecção ou barreiras de segurança presentes (ver 3.3), e nomeadamente com a sua operacionalidade e eficiência/eficácia.

Figura 3.10 – Modelo genérico de Risco de Incêndio

Em termos de **probabilidade de incêndio** pode-se dizer que se trata de um fenómeno aleatório afectado por inúmeros factores, sobre o qual se têm produzido algumas abordagens e teorias. Algumas dessas abordagens têm sido construídas com o objectivo de prever a ocorrência de um incêndio para diferentes tipos de edifícios.

De acordo com Rutstein & Clarke (1979) estima-se a probabilidade de incêndio para diferentes tipos de indústrias, dividindo o número de fogos que ocorrem cada ano pelo número de edifícios em risco (para cada tipo de indústria). Neste caso a probabilidade é não-linear, tendo em conta a área dos edifícios em risco.

Ramachandran (1980) mostra que a probabilidade de início de um incêndio pode ser estimada através da área do edifício e de algumas constantes, conforme a categoria de risco do edifício.

O carácter aleatório e a baixa frequência (felizmente) deste tipo de eventos levou Lie (1998) e Burros (1975) a assumirem que se trata de um Processo de Poisson Homogéneo, podendo a taxa média de início de incêndios por ano ser baseada em informação estatística.

Rahikainen & Keski-Rahkonen (2004) determinaram que as frequências de ignição seguem uma variação de acordo com a semana, mês ou dia da semana, assim como com as horas de cada dia.

De acordo com o estudo de Lin (2005), no período de 1985 a 2001, registaram-se em estabelecimentos industriais, em Taiwan, uma média de 1578 incêndios por ano. Relacionando esses incêndios com a área onde os mesmos ocorreram, que se situa em cerca de 117.809 m^2, dá uma taxa de $1{,}34 \times 10^{-2}$ incêndios/m^2 por ano, a mais alta relativamente a outro tipo de edifícios, como residenciais, lojas, edifícios públicos e outros, também estudados no referido trabalho. Assim conseguir-se-á estimar a probabilidade de incêndio para um determinado tipo de edifício através das correspondentes taxas de incêndio encontradas.

De acordo com Orbeck (1990), em termos de fontes de ignição responsáveis por incêndio ou explosões em edifícios comerciais (citando um relatório da *FM-Factory Mutual Corp.*), pode-se encontrar à cabeça as causas eléctricas, a que correspondem cerca de 271,9 milhões de dólares de perdas por ano.

Tillander (2004) efectuou um estudo de análise de risco de incêndio em edifícios suportada numa base de dados nacional (*Pronto*) sobre acidentes na Finlândia desde 1996, obtendo assim nova informação sobre riscos de incêndio e apresentando métodos quantitativos para avaliação. O uso de informação estatística é, neste caso, um bom meio para tentar caracterizar incêndios. Este estudo centra-se na frequência de ignições, perdas económicas e operação do departamento de segurança nestas situações. A frequência de ignição tem origem no levantamento da área total do piso para cada categoria diferente de edifícios. Os parâmetros e os coeficientes de segurança parciais do modelo foram estimados para três grupos diferentes de edifícios e encontra-se preparado para determinar a frequência de ignição em edifícios com uma área total por piso de 100 a 20.000 m^2. Nesta abordagem distinguem-se os edifícios que possuem sistemas de extinção automática dos restantes. Também se chegou à conclusão que o factor mais importante que afecta o desempenho da força de combate é o tempo que a mesma leva a viajar até ao local do acidente, pelo que uma detecção e uma resposta mais lenta reduzirão significativamente as hipóteses de sucesso. Como consequências do incêndio contabilizam-se as perdas económicas, relacionando as mesmas com a área total do compartimento.

Quanto às **consequências**, e devido à diversidade de tipos de indústria, a sua localização, a sua implantação e as várias políticas de gestão, manutenção e segurança, pode-se afirmar que cada caso é um caso, requerendo também este aspecto uma análise cuidada.

Fontana *et al* (1999) mostram que, segundo um estudo realizado na Suiça no período 1986-1995, ocorreram neste país cerca de 335.000 incêndios em edifícios. Só no cantão de Berna verificaram-se cerca de 1538 incêndios no sector industrial, sendo os prejuízos valorizados em cerca de 66.703 milhões CHF (1 US$=1.48 CHF, à data).

De acordo com outro estudo efectuado na Grã-Bretanha (Ramachandran, 1999), estima-se que por ano morrem cerca de 800 pessoas e ficam feridas cerca de 15.000, relacionados com a ocorrência de incêndios. Em média, por ano, a perda de material directo cifra-se em cerca de 1,2 milhões de libras e material indirecto em 120 milhões de libras. As perdas directas e indirectas devido a incêndios representam na Grã-Bretanha cerca de 0,21% do produto interno bruto do país.

Segundo Shaluf *et al* (2003), e de acordo com o relatório da *United Nations Environmental Program* de 2002, refere-se que nos 12 maiores acidentes em refinarias relacionados com incêndios, o resultado cifra-se em 101 mortes, 111 feridos graves e cerca de 150.000 pessoas evacuadas, não se contabilizando os prejuízos materiais e económicos daí resultantes.

De acordo com Kim *et al* (2002), em 40 casos estudados de incêndios na indústria química entre 1983 e 1997, os prejuízos respeitantes a danos nas instalações ascendem a 1.617 milhões de dólares e com a perda de produção cifra-se em 2.370 milhões de dólares.

Assim, mostra-se de uma forma bastante clara a importância deste tema, justificando o desenvolvimento de um trabalho nesta área, com o objectivo de tentar construir um modelo que de qualquer forma sirva para conhecer e gerir o risco, tendo como objectivo principal a redução do risco potencial de incêndio nas instalações.

3.4.2 – Objectivos das barreiras de segurança contra incêndios

Conforme se pode constatar pela leitura dos pontos anteriores, os sistemas de protecção ou barreiras de segurança existentes numa instalação assumem um papel fundamental na redução do risco, uma vez que podem fazer variar a severidade ou gravidade das consequências de um incêndio, caso este ocorra. No entanto, de nada serve o investimento neste tipo de sistemas se não houver a preocupação de os manter disponíveis e operacionais. Os meios de protecção contra incêndios assumem assim um

papel fundamental, principalmente quando se abordam questões como a eficácia ou eficiência dos mesmos.

Nesta fase convém distinguir os dois conceitos anteriormente referidos. Num contexto de gestão, "eficiência" corresponde à forma e aos meios utilizados na realização de uma actividade, que é tanto mais eficiente quanto menores forem os recursos utilizados na sua concretização (matérias primas, pessoas, dinheiro e tempo). A máxima eficiência é desta forma atingida quando utilizado o mínimo de recursos. A "eficácia" mede o grau de satisfação e o alcance dos objectivos, face aos resultados obtidos. Quanto mais eficaz for uma tarefa, maior o nível dos resultados e maior a satisfação. A máxima eficácia é atingida com o alcance total dos objectivos pré-estabelecidos.

Na prática, a eficácia é sensivelmente simples a medir. Já a eficiência é mais complicada mas advém sobretudo da instauração de novos métodos de produção, da automatização de procedimentos e da tecnologia presente. Assim, ganhos de eficiência traduzem-se geralmente por diminuições de custos.

Esta eficiência dos equipamentos e meios de protecção contra incêndio está directamente relacionada com algumas das várias fases do ciclo de vida desses mesmos equipamentos, nomeadamente com:

- Projecto;
- Ensaio / Comissionamento;
- Exploração;
- Abate ou desmantelamento (sem grande influência, no caso específico).

A eficácia só pode ser medida numa fase específica, que se pretende seja a de maior duração em termos temporais, ou seja:

- Exploração

Nesta fase é que os equipamentos são colocados verdadeiramente à prova, durante os ensaios e simulacros e fundamentalmente perante situações de acidente real. É neste estágio do ciclo de vida dos equipamentos que o papel da manutenção tem especial importância e reflexo no desempenho e no atingir dos objectivos para os quais foram concebidos e instalados.

Dieken (2008) afirma que, por ano, em situações de incêndio, os sistemas de supressão avariam, e que em cerca de um terço das vezes que isso ocorre se deve a uma

inspecção, teste e manutenção inadequada. Nesse artigo é mencionado um estudo do *Edison Electrical Institute* (EEI) onde se refere que num período de 20 anos, devido a erros e omissões relacionados com a manutenção em cerca de 49% dos sistemas de supressão por gás em turbinas de combustão, resultaram prejuízos para a propriedade no valor de 15,9 milhões de dólares.

No que respeita à segurança contra incêndios, diversos sistemas ou barreiras de segurança podem ser estudadas. Podem ser referidos alguns sistemas estáticos, como paredes ou portas corta-fogo ou o estudo de materiais relativamente ao seu comportamento de reacção e resistência ao fogo, ou sistemas dinâmicos, como redes de incêndio armadas (RIA), sistemas de desenfumagem, sistemas automáticos de detecção de incêndios (SADI), sistemas de extinção por espuma ou gases ou sistemas automáticos de extinção (mais conhecidos como redes de *sprinklers*), entre outros. Pode também ser analisado um terceiro tipo de elementos que fazem parte da segurança contra incêndios, mais do foro organizacional, como caminhos de evacuação, iluminação de emergência, sinalética ou planos de emergência.

3.5 – Conclusões do Capítulo

No seguimento do capítulo anterior, o Capítulo III visou definir o que se entende por Risco. Apresentaram-se algumas definições e fez-se referência à normalização relativa a análises de risco.

Mostrou-se como o risco pode ser traduzido pelo produto da probabilidade de ocorrência de um acontecimento indesejável pela severidade ou gravidade das suas consequências. Com base nestes dois factores foi apresentada uma metodologia relativa à avaliação do risco, comparando o risco potencial com o que se pode considerar aceitável, de acordo com um critério de aceitação pré-estabelecido (ALARP, GAMAB, MEM, etc.). De igual forma foi apresentada uma matriz denominada "matriz de risco", habitualmente recorrente quando se analisam potenciais acidentes.

Foram apresentadas algumas metodologias genéricas de análise de risco e introduzido o conceito de barreiras de segurança. Classificaram-se as funções das barreiras de segurança e os sistemas de segurança. Também se mostraram algumas metodologias que permitem efectuar uma avaliação do desempenho das barreiras de segurança.

De uma forma geral, foram descritas as particularidades inerentes aos meios normalmente usados para prevenir, controlar ou mitigar acontecimentos indesejáveis ou acidentes, fazendo referência a conceitos como o Nível de Integridade de Segurança (SIL = *Safety Integrity Level*), Sistemas Instrumentados de Segurança (SIS = *Safety Instrumented Systems*), Probabilidade de Falha quando Solicitado (PFOD = *Probability of Failure On Demand*) ou Análise de Camadas de Protecção (LOPA = *Layer Of Protection Analysis*).

Partiu-se da noção generalizada de risco para particularizar uma temática específica, ou risco específico, nomeadamente o "***Risco de Incêndio***", uma vez que nos capítulos seguintes será dado especial relevo à análise de equipamentos considerados barreiras de segurança, destinados a controlar ou mitigar este tipo de acontecimento. Trata-se de uma área de grande preocupação, havendo a necessidade de se efectuarem estudos e desenvolver novas metodologias de análise, no que respeita à prevenção e protecção deste tipo de eventos.

No presente capítulo fez-se precisamente a diferenciação entre prevenção e protecção, enunciando os factores que contribuem para a existência de risco de incêndio, apontando as medidas de protecção como forma de minimizar a gravidade das consequências.

Apresentou-se um histórico de acontecimentos relacionados com acidentes resultantes da ocorrência de incêndios, de forma a mostrar a importância do tema e algumas metodologias ou abordagens sobre o assunto, quer quanto à probabilidade de ocorrência, como quanto às consequências.

As barreiras de segurança, devido à particularidade de normalmente se encontrarem num estado específico denominado "***dormant***", podem-se considerar especiais do ponto de vista da análise de risco de uma instalação. Assim, pode-se considerar toda a anterior descrição relativa a esta temática como uma introdução e uma ponte para o Capítulo IV.

CAPÍTULO IV

ANÁLISE DE BENS NO ESTADO "*DORMANT*"

4.1 – Introdução

De uma forma geral pode-se considerar que o estado de um bem corresponde à condição em que o mesmo se encontra em determinado momento para cumprir a sua função. De uma forma sintética, podem-se indicar basicamente duas situações relativamente ao estado dos equipamentos:

- Situação de indisponibilidade;
- Situação de disponibilidade.

Por vezes os equipamentos também podem estar parcialmente disponíveis, podendo apenas cumprir parte das funções com que normalmente se encontram capacitados. Por exemplo, se for definido que uma electrobomba deve debitar um caudal de 100 m^3/h ($\pm$10%) e por determinadas razões se registar um caudal de apenas 85 m^3/h, poder-se-á dizer que existe uma falha ou eventualmente afirmar que o referido equipamento se encontra parcialmente avariado, uma vez que se regista efectivamente transferência do fluído, mas não de acordo com os valores especificados.

De qualquer forma, a partir das duas situações básicas inicialmente apontadas, podem-se referir alguns estados complementares, tais como (Pallerosi, 2007d):

- Estado de incapacidade permanente – Estado de um bem caracterizado por o mesmo se encontrar num estado crítico;

- Estado de incapacidade temporária – Estado de um bem caracterizado por este se encontrar em manutenção preventiva, no estado de falha ou de incapacidade por razões externas;
- Estado de capacidade operacional – Estado de um bem caracterizado por este se encontrar no estado de prontidão, de reacção ou de operação efectiva.

Inerente aos estados de incapacidade e capacidade anteriores, ainda podem ser referidas algumas situações particulares, tais como:

- Estado critico – Estado relacionado com condições perigosas e/ou inseguras para as pessoas, avultadas perdas materiais ou danos ambientais graves;
- Estado de manutenção preventiva – Estado em que o bem permanece durante o tempo inerente a acções de manutenção de carácter preventivo;
- Estado de avaria - Estado que resulta da ocorrência de uma avaria e que leva a uma intervenção de manutenção tipo correctiva;
- Estado de incapacidade devido a razões externas – Estado correspondente a um bem que se encontra disponível, mas que por falta de recursos externos se encontra indisponível temporariamente;
- Estado de prontidão – Estado em que o bem se encontra disponível mas não em operação, como é o exemplo de um componente que se encontra em "*standby*", pronto para operar;
- Estado de reacção – Estado relativo ao período de tempo que alguns equipamentos necessitam desde que são activados até atingirem a sua condição plena de operação;
- Estado de operação – Estado onde o bem se encontra a desempenhar correctamente as funções requeridas;

A aplicabilidade destas definições, ou eventualmente de outras, depende de cada equipamento em particular. As situações anteriormente referidas podem ser esquematizadas e apresentadas conforme Figura 4.1.

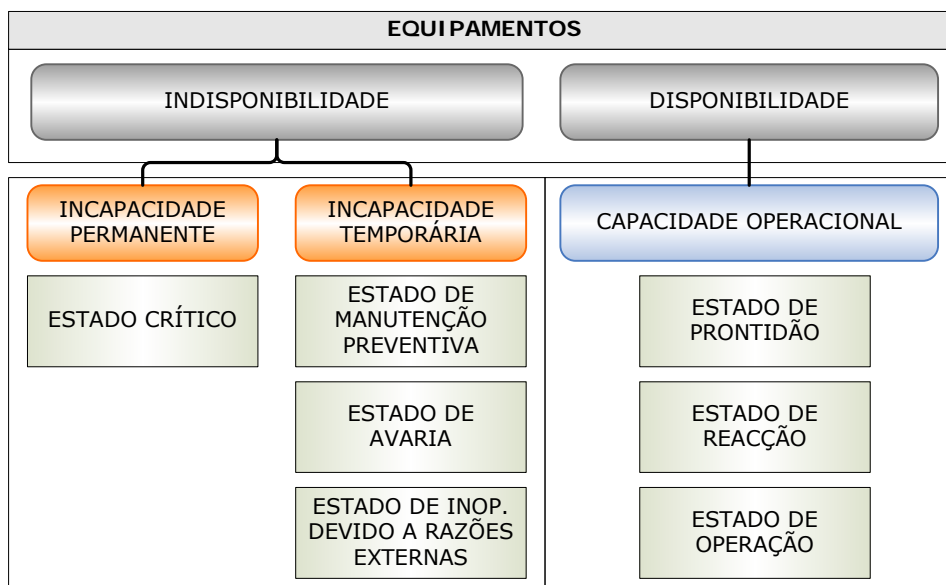



Figura 4.1 – Possibilidade de estados de um bem

Outro tipo de classificação, não muito distinto do anteriormente referido, é apresentado na NP EN 13306 (2007), onde os diferentes estados de um bem são apresentados de acordo com a Figura 4.2.

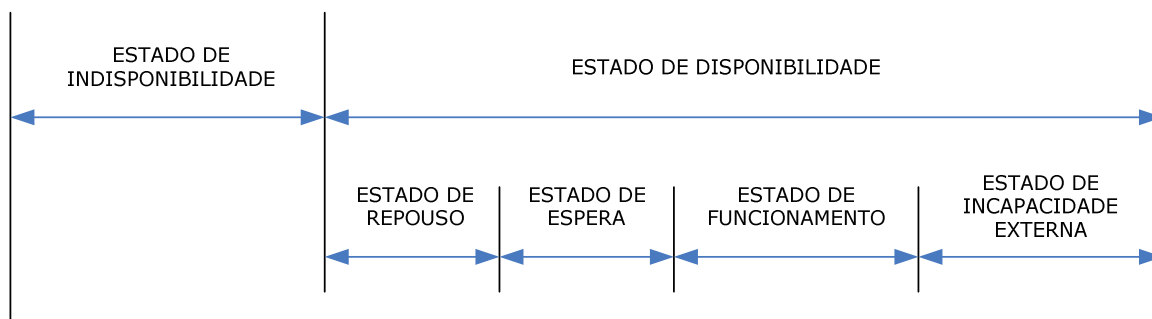



Figura 4.2 – Exemplo dos diferentes estados de um bem

Na referida norma, cada um estados é definido da seguinte forma:

- Estado de indisponibilidade – Estado de um bem caracterizado por um estado de falha ou por uma eventual capacidade para desempenhar uma função requerida durante a manutenção preventiva;
- Estado de disponibilidade – Estado de um bem caracterizado pelo facto que pode cumprir uma função requerida, assumindo que o fornecimento de recursos externos, eventualmente necessários, está assegurado;

- Estado de repouso – Estado de um bem disponível quando não está em funcionamento durante um tempo em que não é requerido;
- Estado de espera - Estado de um bem disponível quando não está em funcionamento durante um tempo em que é requerido (diferente do termo "*funcionamento em vazio*");
- Estado de funcionamento – Estado de um bem que cumpre a função requerida;
- Estado de incapacidade externa - Estado de incapacidade de um bem disponível, por falta de recursos externos necessários ou que não está disponível devido a acções programadas que não sejam de manutenção.

De uma forma geral, pode-se dizer que os bens sujeitos à análise de falhas e a estudos de fiabilidade, manutibilidade, disponibilidade e segurança podem encontrar-se em vários estados de funcionamento ao longo do seu ciclo de vida, de acordo com as suas características de projecto, de exploração e de manutenção. Do ponto de vista dos bens que se encontram com capacidade operacional, podem-se definir basicamente dois tipos de situações, nomeadamente:

- Bens em operação;
- Bens em não-operação.

Relativamente ao primeiro tipo, podem-se aplicar os conhecimentos teóricos tradicionais relacionados com o tipo de análise que se pretenda efectuar (fiabilidade, manutibilidade, disponibilidade e segurança), sendo frequentemente encontrados diversos estudos nessas matérias. Quanto aos bens que se encontram em não-operação, quer por simplesmente se encontrarem armazenados, ou eventualmente se encontrarem instalados em "*standby*" ou num estado adormecido (*dormant*), já a quantidade de estudos não é tão vasta.

Podem ser referidos alguns trabalhos, como por exemplo um estudo (Wu & Clements-Croome, 2007) onde se mostra como estabelecer as melhores políticas de "*burn-in*" para produtos no estado "*dormant*", dando como referência equipamentos que são instalados em edifícios na fase de construção e que não funcionam até que se dê o comissionamento do edifício. De qualquer forma, é necessário dar garantia dos equipamentos durante esse período. O desenvolvimento de políticas óptimas de "*burn-in*" para esses produtos é importante quando se analisam os custos no período de garantia, sendo também apresentados dois exemplos numéricos onde se comparam os custos totais, em termos médios, conforme a política adoptada.

Outro estudo (Wu & Li, 2007) refere o período de garantia de produtos no estado "*dormant*", numa vertente de análise de custos, tendo em conta os custos de manutenção preventiva e manutenção correctiva durante esse período, e considerando três tipos de falhas típicos em produtos no modo adormecido (*dormant*).

Hokstad & Frovig (1996) apresentam modelos para o mecanismo de avarias que levam a falhas por degradação e falhas críticas[9], e mostram como determinar os estimadores para a intensidade das avarias, visando fundamentalmente as falhas ocultas, características de bens no estado "*dormant*" ou em "*standby*". Nestes modelos também é possível quantificar a redução na taxa de avarias críticas, reparando atempadamente as avarias consideradas por degradação.

Em algumas situações os equipamentos podem ficar inactivos no terreno (sujeitos a vários factores ambientais) ou noutro local (possivelmente à espera de manutenção). Durante estes períodos os sistemas também podem entrar em contacto com diversos esforços, que podem ser naturais (ex. humidade, pó, temperaturas altas ou baixas, etc.) ou induzidos, devido a erro humano (ex. mau manuseamento). Um sistema pode estar situado em vários ambientes de não-operação durante o seu ciclo de vida. Alguns desses ambientes devem ser analisados, devido à possibilidade de poderem causar avarias aos sistemas, enquanto outros podem ser de importância negligenciável.

4.2 – *Dormant State*

Nesta fase convém clarificar o que se entende por bens no estado "*dormant*", ou adormecido, e realçar as diferenças relativamente a outros equipamentos que normalmente se encontram em serviço considerado contínuo, ou quase contínuo.

De acordo com um estudo do RAC (*Rome Air Development Center*) (Seman *et al*, 1988), os modos de não-operação podem ir desde o simples armazenamento até ao estado de prontidão e alerta em que se pode encontrar um determinado bem. Reportando-se o referido estudo a equipamentos militares, pode-se constatar que o estado "*dormant*" corresponde a uma percentagem elevada de tempo, relativamente a todo o ciclo de vida

---

[9] Neste estudo, aparecem os termos "*critical*", "*degraded*" e "*incipient*", referindo-se a falhas que implicam a perda total da função principal, à degradação em alguma parte do bem (garantindo no entanto o cumprimento da função) e a falhas que poderão ser ignoradas, respectivamente.

dos equipamentos. Como este estado e os seus efeitos nem sempre são considerados durante as fases de projecto, o documento anteriormente referido foi preparado para servir como guia nessa fase do ciclo de vida, com o objectivo de mitigar os efeitos produzidos em equipamentos electrónicos por estes se encontrarem num estado tipo "*dormant*", e assim melhorar a fiabilidade, manutibilidade e capacidade de teste[10] deste tipo de sistemas militares.

Para evitar possíveis confusões quanto ao que realmente se entende por "*dormant*", e diferenciar esta característica daquela em que um bem que se encontra pura e simplesmente armazenado, apresenta-se de seguida uma descrição mais pormenorizada da diferença entre o estado referido como de "*dormancy*", e o de "*storage*" (Carchia, 1999) (Pecht & Pecht, 1995).

"*Dormancy*" é definido como um estado no qual o equipamento está na sua configuração operacional normal e ligado, mas não em operação. Para efeitos de testes, o equipamento no estado "*dormant*" poderá ser ligado e desligado ciclicamente. Durante o período "*dormant*", as tensões eléctricas presentes em condições de operação são normalmente reduzidas ou eliminadas;

"*Storage*" é definido como o estado no qual o sistema, subsistema ou componente está totalmente inactivo e permanece numa área de armazenagem. Normalmente o produto pode ter que ser desembalado e ligado a uma fonte de energia para ser testado.

Quanto aos bens que se encontram armazenados são referidos dois estudos. Um desses estudos (Martinez, 1984) aborda a questão da fiabilidade de equipamentos electrónicos que poderão avariar antes ou no momento em que são colocados em serviço após longo período de armazenagem, mostrando a importância dos testes efectuados na tentativa de manter a sua fiabilidade inerente.

O outro estudo (Ito & Nakagawa, 2000) refere-se a mísseis e componentes de avião armazenados durante um longo período e que, para garantia da sua fiabilidade, são sujeitos a testes periódicos. Neste estudo, apresenta-se o compromisso entre os custos inerentes à realização desses testes com os custos referentes a uma revisão geral,

[10] Esta designação provem do termo anglo-saxónico "*testability*", usado normalmente no campo informático no processo e desenvolvimento de software (ISO/IEC 12207), e refere-se à maior ou menor facilidade, e consequente rapidez, com que um sistema pode ser testado, com vista a aferir o seu estado funcional.

necessária na eventualidade de não se realizarem inspecções com a frequência indicada, e assim a fiabilidade chegar a valores inaceitáveis.

Os estados "*dormant*" e "*storage*", em conjunto com um terceiro modo, designado de "*standby*", são situações bastante comuns de encontrar durante a vida de muitos sistemas. No caso de sistemas no estado "*dormant*", a solicitação dá-se com base numa informação (sonda, pressostato, etc.), enquanto nos sistemas "*standby*", a solicitação ocorre quando o sistema ou componente primário avaria, embora nesta situação também seja normalmente necessário haver uma informação de avaria do componente primário (através do detector-comutador ou sensor-comutador). A principal diferença entre o estado "*dormant*" e o estado "*standby*" reside no facto de na primeira situação (*dormant*) não existir um sistema primário e na segunda ("*standby*") ter de o haver. Na maior parte dos casos tem-se também de considerar que alguns sistemas em "*standby*" se encontram numa situação "*dormant*".

Quanto a componentes em "*standby*" podem ser indicados alguns estudos referentes ao cálculo da sua fiabilidade, podendo, no enquadramento do presente trabalho, ser referido o trabalho realizado por Courtois & Delsarte (2006), onde se apresenta um modelo para determinar a frequência óptima para a realização dos testes e manutenção de componentes redundantes. Através do modelo desenvolvido mostra-se que quanto maior for a frequência de inspecção, menor é a probabilidade de uma falha oculta ocorrer entre inspecções sucessivas, tendo-se por objectivo confrontar este aumento da fiabilidade com a indisponibilidade das redundâncias, motivada pelo tempo necessário à realização dessas inspecções. Neste estudo também se assume que as inspecções são perfeitas.

De igual forma, é referido outro estudo (Motta & Colosimo, 2002) onde se determina a frequência para a manutenção preventiva de unidades em "*standby*" com a apresentação de uma aplicação prática sobre relés de uma instalação produtora de energia eléctrica no Brasil. Neste trabalho, os autores mostram como as falhas ocultas de bens em "*standby*" levam a maiores dificuldades na determinação da periodicidade para efectuar a manutenção preventiva. Normalmente esta periodicidade é baseada na experiência e julgamento dos técnicos e engenheiros de manutenção, com alguma subjectividade. No trabalho desenvolvido pelos autores anteriormente citados, relativo a relés de protecção de um sistema de transmissão e distribuição, refere-se que relativamente às falhas ocultas, são apontados basicamente dois modos:

- Falha na operação, na presença de uma solicitação operacional, também designada por falha operacional;

- Operação desnecessária, na ausência de qualquer solicitação, designada por falha segura (não estudadas nesse trabalho).

Os autores referem também que normalmente os estudos de fiabilidade de sistemas de protecção apenas têm em consideração as falhas em serviço, subestimando assim a fiabilidade do sistema. Desta forma, para se obterem resultados mais reais, as falhas ocultas deverão também ser consideradas nestes estudos, uma vez que este tipo de equipamentos (de protecção) tende a ficar no estado de "*standby*" por largos períodos de tempo.

Assume-se que as anomalias encontradas num sistema aquando das inspecções são resolvidas, tipificando modelos de reparação perfeita, ficando o sistema num estado designado na literatura anglo-saxónica como "*as good as new*". Também se assume que os tempos até à avaria seguem uma distribuição exponencial, justificada em termos teóricos por um processo de renovação. Este tipo de processo tem lugar quando um número de situações individuais combinam para formar um processo global, denominado um processo super-imposto. O processo global tende para um Processo de Poisson Homogéneo, mesmo que as variáveis individuais não sejam necessariamente independentes e identicamente distribuídas (Motta & Colosimo, 2002).

Zang *et al* (2006) referem uma metodologia de cálculo para a disponibilidade e fiabilidade de sistemas em "*standby*", tendo em conta que os mesmos possuem taxas de avaria e de reparação diferentes. Neste trabalho, os autores introduzem o conceito de "*dormant failure*", referindo que ao introduzir-se redundâncias para melhorar a fiabilidade e disponibilidade de um sistema, três tipos de situações podem ocorrer relativamente às propriedades dessas redundâncias (*standby*), nomeadamente:

- *Cold standby* – implica que os componentes inactivos têm uma taxa de avarias nula e não podem avariar neste estado;
- *Hot standby* – implica que um componente inactivo tenha a mesma taxa de avarias que um componente em operação;
- *Warm standby* – é um caso intermédio que implica que um componente inactivo tenha uma taxa de avarias com um valor entre um *hot standby* e um *cold standby*. É a este último caso que os autores denominam de "*dormant failure*".

Quando se fala de equipamentos de protecção, designados como barreiras de segurança, normalmente as suas falhas apenas são reveladas aquando da solicitação (situação real ou teste). Só nesta fase se poderá iniciar um processo de reparação ou troca de

componentes, se tal for possível e viável. Badía *et al* (2002) mostram que as falhas ocultas permanecem desconhecidas desde que não se efectuem inspecções ou testes, e que este tipo de falhas normalmente ocorre em equipamentos armazenados, unidades em "*standby*" ou sistemas que raramente funcionam, como os sistemas de segurança. A excepção encontra-se nos casos em que se monitorizam alguns sistemas, podendo actuar-se de imediato, assim que se detecte alguma anomalia.

4.3 – As barreiras de segurança e o estado "*Dormant*"

Relativamente às barreiras de segurança constata-se que uma grande quantidade de sistemas críticos de segurança (e não só) passa a maior parte da sua vida num estado não operativo. Esta noção de não-operação é caracterizada pela existência de componentes ou sistemas pertencentes a um equipamento funcional, onde ocorre uma redução ou a eliminação dos esforços mecânicos e/ou eléctricos (quando comparados com a condição normal de operação).

Harris (1980) compilou uma lista de valores típicos para o tempo dispendido no estado de não-operação de vários tipos de equipamentos. Esta lista, conforme Tabela 4.1, demonstra que o estado de não-operação pode significar uma percentagem considerável da vida de alguns sistemas.

Tabela 4.1 - *Valores típicos em percentagem de tempo de calendário para equipamentos no estado de não-operação*

Aplicações Domésticas	
Televisões	75%
Equipamentos eléctricos de cozinha	97%
Carros	
Uso pessoal	93%
Uso público (táxis)	38%
Equipamento Profissional	
Calculadoras pessoais	98%
Fotocopiadoras de pequena dimensão	>75%
Equipamento de teste electrónico	>90%
Equipamento Industrial	
Equipamento de segurança	98%
Energia *standby* (gerador de emergência)	>90%
Válvulas	>75%
Ar condicionado	50-80%
Equipamento de teste local	99%

Relativamente a barreiras de segurança no estado "*dormant*" importa também realçar que poderão ocorrer outro tipo de avarias, designadas por "avarias não perigosas" ou "avarias seguras", que resultam da actuação intempestiva dessas barreiras sem que se tenha observado a ocorrência do acontecimento potencialmente perigoso. Devido à sua criticidade ser praticamente nula, nomeadamente no que se refere à severidade ou gravidade das suas consequências, este tipo de avarias não são analisadas no presente estudo.

De acordo com os conceitos enunciados no Capítulo II, a disponibilidade pode ser vista de três formas:

1. Como a probab. do bem funcionar quando solicitado;
2. Como a probab. do bem se encontrar a funcionar num determinado tempo "*t*";
3. Como a fracção do tempo total em que o bem consegue realizar a sua função.

Quando aplicada aos bens no estado "*dormant*", pretende-se fundamentalmente que os mesmos funcionem cada vez que forem solicitados, e que posteriormente a esta fase, que o sistema seja fiável durante um determinado tempo ou missão. Quando se trata de equipamentos de protecção (segurança), pode-se afirmar que neste caso concreto o sistema reage a um acontecimento indesejável, e actua para prevenir uma situação perigosa. Se esse mesmo sistema estiver numa situação de incapacidade temporária ou permanente quando for solicitado, podemos então afirmar que ele se encontra indisponível.

A maior parte dos sistemas de segurança encontra-se no estado "*dormant*", operando apenas se necessário, ou seja, não se encontra em operação contínua. Devido à sua aplicação e importância no sector industrial, onde o risco é particularmente elevado, justifica-se um cuidado especial no tratamento deste tipo de sistemas. Será sobre os bens que se encontram neste estado que o presente capítulo irá incidir, desenvolvendo alguns conceitos e demonstrando a sua aplicabilidade.

A periodicidade com que os testes são efectuados é um factor de extrema importância a ser considerado. Quanto menor for o intervalo de tempo entre testes mais cedo se descobrem as potenciais falhas ocultas (*hidden failures*), embora por outro lado se possam também induzir algumas (ex. erro humano durante uma acção de manutenção). Além deste factor, também têm que se considerar maiores custos com a manutenção,

devido ao aumento da sua frequência. O presente trabalho pretende abordar algumas destas questões na óptica da análise a barreiras de segurança no estado "*dormant*".

4.4 – Metodologias de análise

Enquanto a literatura mais comum se centra na fiabilidade em serviço, convém não esquecer que, de acordo com os parágrafos anteriores, o estado de não-operação também deve requerer a atenção dos projectistas e analistas de sistemas. Os sistemas projectados para operar com alta fiabilidade não funcionam necessariamente bem após largos períodos de exposição em ambientes de não-operação, e há que ter isso em conta. Assim, quando se trata de equipamentos nestas circunstâncias, os assuntos relacionados com as suas avarias (ou falhas) necessitam também de ser analisados e tidos em consideração na fase de projecto e exploração do seu ciclo de vida.

Raras vezes existem dados de campo específicos, a partir dos quais se pode determinar a fiabilidade dos bens no estado "*dormant*". Destaca-se pela positiva o caso da indústria automóvel onde a informação referente a determinadas partes pode ter sido recolhida em modelos mais antigos de viaturas e posteriormente aproveitada para novos modelos, desde que os componentes sejam suficientemente idênticos e a operar em condições similares.

Existem outras abordagens sobre os componentes usados numa situação de redundância, onde se associa um factor de adormecimento ou "*dormancy factor*" (α), que varia entre os valores zero e um (inclusive) (Carchia, 1999). Este será então um factor multiplicativo à taxa de avarias calculada para esse componente, quando numa situação de operação, e que pode ser determinado em função das condições ou factores ambientais em que o mesmo se encontra.

Se este factor assume o valor zero (α=0), o componente sobressalente designa-se por "*cold spare*". Um "*cold spare*" não pode avariar antes de entrar em serviço. Se o factor tem o valor unitário (α=1), chama-se ao sobressalente um "*hot spare*", podendo avariar com uma taxa idêntica a um componente similar que se encontre em serviço. A um componente cujo valor do factor de adormecimento se refere a qualquer situação intermédia entre zero e um designa-se por "*warm spare*". Este último tipo de componente pode avariar antes de entrar em serviço, mas com uma taxa inferior à de um componente em funcionamento (Meshkat *et al*, 2000).

Como visto anteriormente (Tabela 4.1), os referidos sistemas de segurança passam a maior parte da sua vida (98%) num estado "*dormant*". A fiabilidade deste tipo de bens é crucial, uma vez que quando solicitados, em resultado da sua correcta operação poderão estar em causa o destino da vida de muitas pessoas, a integridade das instalações, a continuidade de actividades ou a existência de danos ambientais graves. Quando a actuação destes sistemas é necessária, por qualquer eventualidade, é importante que funcionem sem avarias!

De acordo com Meshkat *et al* (2000), a análise de fiabilidade de sistemas de segurança, como por exemplo sistemas automáticos de extinção de incêndios (sprinklers) ou outros sistemas de protecção, requer que tenhamos em consideração dois tipos de comportamento em termos de falhas, nomeadamente:

- Falha na solicitação, ou quando solicitado;
- Falha durante a operação (*in service*).

Isto significa que o sistema, que normalmente se encontra num estado "*dormant*", poderá se encontrar em falha quando solicitado ou, uma vez iniciado o seu funcionamento, poderá avariar durante a operação (ou missão).

A falha do sistema no arranque, quando tal é necessário, é um indicador da sua indisponibilidade quando solicitado (*on demand*), enquanto a falha que ocorre após o início do funcionamento corresponderá à sua probabilidade de falha (complementar da fiabilidade). Tipicamente, neste tipo de sistemas, os componentes considerados activos não poderão ser reparados durante o período em que se encontram a ser solicitados.

A probabilidade de falha quando solicitado (PFOD – *Probability of Failure On Demand*), ou a indisponibilidade do sistema, depende das características de falha dos seus componentes de suporte (ou de arranque), enquanto estes se encontram no já referido modo "*dormant*" (adormecido).

Estes componentes de suporte devem ser testados, ensaiados ou ter acções de manutenção periodicamente, enquanto permanecerem nesse estado de não actividade, para que se detectem as já referidas falhas ocultas (*hidden failures*). Uma vez dado o arranque do sistema, é frequente assumir que estes componentes de suporte não irão provocar a avaria do sistema quando em funcionamento activo. Por outro lado, a

probabilidade de avaria durante a operação depende das características de falha dos componentes activos durante todo o período em que se encontram a ser solicitados.

A fiabilidade global do sistema refere-se à probabilidade do sistema continuar disponível após o arranque, e alcançar o sucesso da missão (operação) enquanto for solicitado. A probabilidade de falha quando solicitado (PFOD = *Probability of Failure On Demand*) é considerado um assunto fulcral no estudo de bens no estado "*dormant*". No entanto, de nada serviria obter sucesso nessa fase se depois o equipamento não cumprisse a sua missão.

Para se conduzir uma análise de fiabilidade neste tipo de sistemas, ter-se-á que analisar cada uma destas fases. A primeira refere-se ao modo "*dormant*", enquanto a segunda diz respeito ao sistema quando este se encontra em operação (*in service*). Isto requer uma análise de disponibilidade dos subsistemas de suporte e uma análise de fiabilidade dos componentes activos durante a operação, respectivamente. A Figura 4.3 mostra o enquadramento desta metodologia.

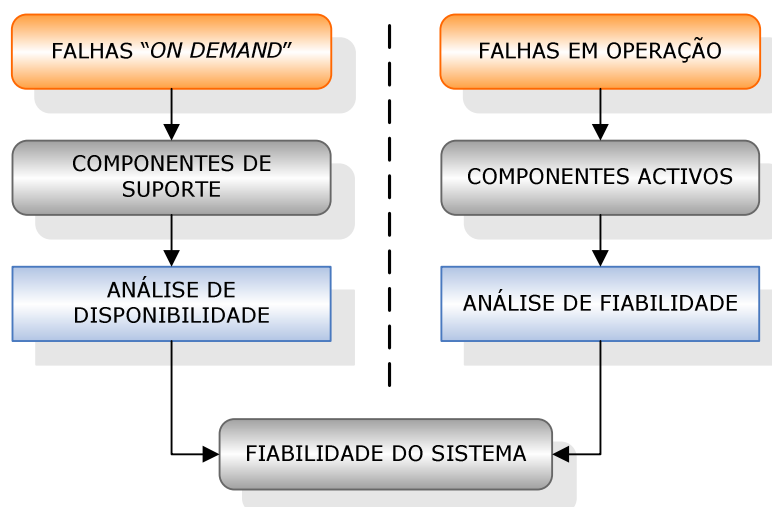



Figura 4.3 – Metodologia de Análise a Sistemas tipo *"Dormant"*

Tal como referido anteriormente, quando se falou sobre redundâncias, também algumas abordagens nesta área apontam para que o estudo de bens no estado "*dormant*" e de bens em funcionamento activo seja efectuado da mesma forma, apenas com a introdução de factores de correcção nos valores referentes às taxas de avarias destes últimos, ou seja, usar as taxas de avarias dos bens em operação regular, onde existe um maior conhecimento e menos incerteza, e de acordo com a aplicação de um factor de depreciação da taxa de avarias, tabelado, determinar a taxa de avarias de um bem

semelhante, mas que se encontre numa aplicação onde seja considerado como "*dormant*" (The Rome Laboratory, 1993).

Esta metodologia pode ser discutível, uma vez que a comparação não é assim tão linear, podendo em alguns casos específicos até ser inversa, como é o exemplo dos vedantes e empanques, cuja taxa de avarias com o bem em funcionamento é menor do que com o mesmo em repouso. Outra razão para não concordar plenamente com a abordagem anterior prende-se com o facto de que muitos dos componentes que se encontram no estado "*dormant*" não intervêm ou não têm um comportamento idêntico quando em serviço.

Nas barreiras de segurança, a ocorrência de uma avaria pode ter consequências catastróficas, uma vez que o tempo necessário para qualquer eventual processo de restauração ou recolocação no seu estado funcional implica o concretizar da situação potencialmente perigosa que a barreira de segurança deveria evitar.

4.5 – Análise da indisponibilidade

Os principais contribuintes para a indisponibilidade de um sistema de segurança derivam genericamente de (Zio, 2007):

- Falhas ocultas – Quando um bem no estado "*dormant*" (ou em "*standby*") avaria, sem que obtenhamos essa informação. O sistema prossegue o seu estado sem avisar da ocorrência da avaria até que um teste seja realizado ou o bem seja requerido para funcionar;
- Manutenção preventiva ou teste – Quando um bem é retirado (ou não) do sistema porque tem que ser testado ou sujeito a manutenção preventiva;
- Reparação – Quando o bem se encontra indisponível devido a se encontrar em reparação, aplicado a bens no estado "*dormant*", quando monitorizados.

Destes três factores, pode-se referir que as falhas ocultas são aquelas que mais preocupam os responsáveis pela gestão dos activos, já que as situações relativas a manutenção preventiva, testes, ensaios e reparações são conhecidas e normalmente controladas.

Se por coincidência ocorrer em simultâneo com estas actividades uma solicitação do sistema de segurança, o equipamento poderá na maior parte das vezes ser

disponibilizado para cumprir a sua função. Um teste ou ensaio poderá ser interrompido quase instantaneamente pelos técnicos que se encontram no local. Normalmente para um bem monitorizado que avarie, procede-se à sua substituição, ou são criadas condições alternativas para que o risco esteja controlado.

Tal como referido no Capítulo II, quando se trata de componentes não reparáveis, os mesmos funcionam até que a primeira avaria ocorra. A probabilidade de no instante "*t*" o componente não se encontrar a funcionar é igual à probabilidade de falha antes desse tempo "*t*", ou seja, a probabilidade acumulada de falha [*F(t)*] (Zio, 2007). Assim, a indisponibilidade instantânea de um componente não reparável é igual à sua função acumulada de falha:

$$q(t) = F(t) \tag{4.1}$$

Logo, a sua disponibilidade será dada por:

$$a(t) = 1 - q(t) \Leftrightarrow R(t) \tag{4.2}$$

De referir que no caso de bens reparáveis monitorizados continuamente se assumir que a sua reparação se inicia logo após a ocorrência da avaria. Nesta situação, é necessário também definir o modelo probabilístico que descreve a duração do processo de reparação, onde [*g(t)*] representa a função densidade de probabilidade de reparação ou recolocação em serviço[11].

4.5.1 – Falhas ocultas

Como referido anteriormente, os sistemas de segurança encontram-se normalmente numa situação adormecida (*dormant*) até à ocorrência do acidente na instalação, altura em que são solicitados para operar. A única forma de ter conhecimento da existência de qualquer avaria em componentes não monitorizáveis será através da realização de testes ou ensaios, onde as falhas ocultas serão reveladas. Para um bem nestas condições, sujeito a testes ou ensaios periódicos, a indisponibilidade instantânea é uma função periódica do tempo. Neste caso, podemos recorrer à indisponibilidade média como

[11] Ver Capítulo II – Conceito RAMS – 2.4

indicador de desempenho. O seu cálculo, para um período de tempo "T" é dado por (Zio, 2007):

$$Q(T) = \frac{1}{T} \cdot \int_0^T q(t).dt = \frac{\overline{downtime}}{T} \quad (4.3)$$

onde "*downtime*" corresponde ao tempo médio que o sistema está indisponível durante o tempo "*T*". Para ilustrar o acima referido, considere-se um caso simples de indisponibilidade de um sistema relacionado com falhas aleatórias (ocultas) que podem ocorrer em qualquer momento com um valor constante de taxa de avarias (λ). Se assumirmos também que o tempo referente aos procedimentos de manutenção e teste é instantâneo, a disponibilidade (instantânea) no intervalo entre testes (τ) coincide com a fiabilidade porque o bem não se encontra monitorizado entre dois tempos sucessivos de manutenção, ou seja, entre:

$(k-1).\tau$ e $k.\tau$ com (k=1, 2, …).

A Figura 4.4 representa a disponibilidade instantânea de um bem sujeito a testes e manutenção com uma periodicidade "τ", assumindo que o mesmo fica "*as good as new*" após o correspondente teste ou manutenção. De acordo com este pressuposto todos os intervalos entre testes são idênticos do ponto de vista estocástico.

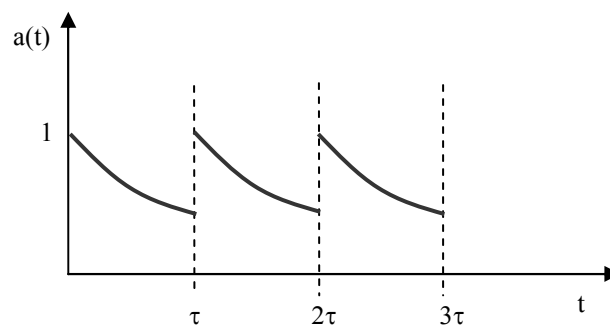



Figura 4.4 – Disponibilidade instantânea de um componente sujeito a testes e manutenção

Para ajudar a compreender o cálculo da indisponibilidade média veja-se a Figura 4.5, que mostra o comportamento genérico de um componente, onde "X(t)" representa o conjunto de estados possíveis (1=operacional e 0=avariado).

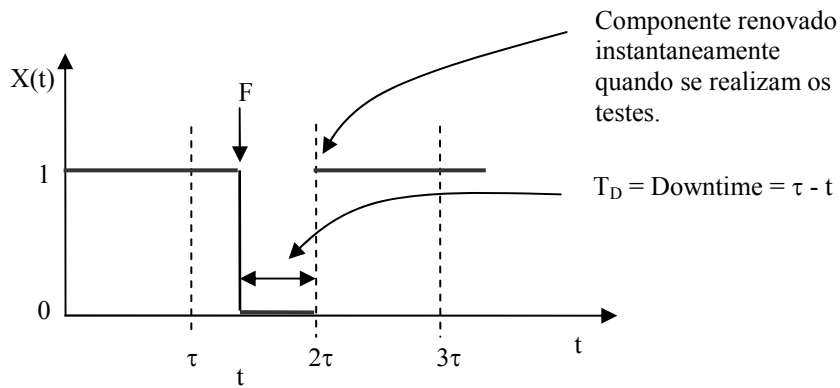



Figura 4.5 – Variável indicadora do estado de um componente

A indisponibilidade média em cada período "τ", é por definição:

$$Q(\tau) = \frac{\overline{downtime}}{\tau} = \frac{\overline{T}_D}{\tau} \tag{4.4}$$

sendo o tempo médio $\overline{T}_D$ dado por:

$$\overline{T}_D = \int_0^{\tau} (\tau - t).f(t).dt \tag{4.5}$$

Integrando por partes:

$$\overline{T}_D = \int_0^{\tau} F(t).dt \tag{4.6}$$

Logo:

$$Q(\tau) = \frac{\overline{T}_D}{\tau} = \frac{\int_0^{\tau} F(t).dt}{\tau} \tag{4.7}$$

Sendo a sua complementar disponibilidade média[12] dada por:

---

[12] De acordo com a expressão (2.22)

$$A(\tau) = \frac{\overline{T}_U}{\tau} = \frac{\int_0^{\tau} R(t).dt}{\tau} \qquad (4.8)$$

onde $\overline{T}_U$ corresponde ao tempo médio de "*uptime*" no período τ.

As expressões (4.7) e (4.8) são precisamente as definições da indisponibilidade e disponibilidade média, respectivamente, durante um período de tempo "τ". Assim, para o cálculo destes indicadores pode-se determinar a sua função de distribuição acumulada de falha ou probabilidade de sucesso e depois aplicar as expressões matemáticas anteriores.

Se os tempos até à avaria do bem reparável estão exponencialmente distribuídos, tem-se:

$$F(t) = 1 - e^{-\lambda.t} \qquad (4.9)$$

Para o caso específico em que, para valores de taxas de avarias e tempos, se obtem:

$$\lambda.t \leq 0{,}10$$

A função de distribuição acumulada de falha pode ser calculada aproximadamente por:

$$F(t) = 1 - e^{-\lambda.t} \cong \lambda.t \qquad (4.10)$$

E a respectiva indisponibilidade média, recorrendo à expressão (4.7), determinada por:

$$Q(\tau) = \frac{\int_0^{\tau} F(t).dt}{\tau} = \frac{\int_0^{\tau} \lambda.t.dt}{\tau} = \frac{1}{2}.\lambda.\tau \qquad (4.11)$$

Com esta conclusão, e de forma intuitiva, podemos esperar que um bem reparável com taxa de avarias constante falhe a meio do período entre testes consecutivos.

De acordo com outro trabalho (Andrews & Moss, 2002), a indisponibilidade média [$Q(\tau)$] de um sistema de segurança, também referida nesse estudo como fracção de tempo

indisponível (FDT = *Fractional Dead Time*), pode ser determinada pela seguinte expressão:

$$Q(\tau) = \frac{\lambda.\tau}{2} + \lambda.\tau_R \qquad (4.12)$$

$$Q(\tau) = \lambda.\left(\frac{\tau}{2} + \tau_R\right) \qquad (4.13)$$

onde:

λ = Taxa de avarias (falhas ocultas) do bem, considerada constante

τ = Intervalo de tempo entre testes ou ensaios

τ_R = Tempo médio de reparação do bem

A expressão (4.13) tem significado desde que se garanta que qualquer avaria pode ocorrer em qualquer altura (tempo), e assim o tempo médio para a avaria encontra-se a meio do intervalo de tempo estipulado para a manutenção (teste, ensaio, inspecção).

Parte-se também do pressuposto que qualquer avaria detectada aquando dos testes, ensaios ou inspecções é resolvida, encontrando-se todo o sistema operacional no fim da acção de manutenção.

Nos sistemas de segurança, além do tempo médio de reparação (τ_R) ser normalmente bastante inferior ao intervalo de tempo entre testes ou ensaios (τ), em situações reais de solicitação não deveremos considerar a reparação, tal como justificado anteriormente. Partindo desta hipótese, a expressão para o cálculo aproximado da indisponibilidade média do sistema pode agora apresentar-se da seguinte forma:

$$Q(\tau) = \frac{\lambda.\tau}{2} \qquad (4.14)$$

Conforme se pode verificar, a expressão anterior encontra-se coerente com a expressão (4.11).

Para validar a equação anterior podemos referir também outro trabalho (Kumamoto, 2007), onde se menciona que a contribuição das avarias perigosas não detectadas (λ_{DU}) após um teste ou ensaio pode ser quantificada através da probabilidade de falha do sistema (reparável) quando solicitado, numa estrutura simples "*um de um*" (Q_{1oo1}),

definida como uma probabilidade de falha média, ou indisponibilidade (*Q*) num intervalo de tempo (τ) correspondente ao intervalo entre testes, tal que:

$$Q_{1oo1} = \lambda_{DU} . \left(\frac{\tau}{2} + MTTR \right) + \lambda_{DD} . MTTR \quad (4.15)$$

Onde:

λ_{DU}= Taxa de avarias perigosas não detectadas

λ_{DD}= Taxa de avarias perigosas detectadas

MTTR = Tempo médio de reparação (*Mean Time To Repair*)

τ = Intervalo de tempo entre ensaios (testes, inspecções)

A equação anterior coincide também com outro estudo, apresentado pela *International Electrotechnic Comission* (IEC) (IEC:61508, 1998).

Se continuarmos a assumir que λ_{DD}=*MTTR*=0, a expressão anterior reduz-se novamente a:

$$Q_{1oo1} = \frac{\lambda_{DU} . \tau}{2} \quad (4.16)$$

Estando novamente em sintonia com as expressões (4.11) e (4.14).

De acordo com outro trabalho analisado (US Nuclear Regulatory Comission, 1981), para sistemas sujeitos a testes periódicos (τ), e partindo do pressuposto que qualquer falha detectada durante os testes é imediatamente solucionada (100% dos modos de falha são detectados), a indisponibilidade varia desde o valor zero, no instante imediatamente a seguir à realização do teste, até ao valor mais elevado (indisponibilidade $\cong \lambda\tau$) registado no instante imediatamente inferior à realização do próximo teste. Como a distribuição exponencial pode ser aproximadamente uma função linear, a indisponibilidade média [*Q(t)*] entre testes é aproximadamente:

$$Q(t) = \frac{\lambda . \tau}{2} \quad (4.17)$$

No entanto, para as equações anteriores (4.11), (4.14), (4.16) e (4.17), e para algumas combinações da taxa de avarias e intervalo de tempo entre inspecções, podem-se obter

valores de indisponibilidade média superior à unidade (>1,0). Esta situação deve-se à aproximação assumida em (4.10). Por forma a estabelecer um sistema coerente e aplicável a todos os casos práticos, ter-se-á que encontrar uma expressão mais concreta, que permita obter um valor para a indisponibilidade que se situe no intervalo 0<*Q(t)*<1.

Como não se considera a reparação dos bens nos períodos entre as acções de manutenção programada (testes ou ensaios), pode-se então apresentar de uma forma mais correcta a indisponibilidade média considerando o primeiro intervalo (entre $t=0$ e $t=\tau$). Para tal recorre-se e desenvolve-se a expressão (4.9).

$$Q(t) = \frac{1}{\tau}.\int_0^{\tau}\left(1-e^{-\lambda.t}\right)dt \tag{4.18}$$

$$Q(t) = \frac{1}{\tau}.\left[\tau + \frac{e^{-\lambda.\tau}}{\lambda}\right]_0^{\tau}$$

$$Q(t) = \frac{1}{\tau}.\left[\tau + \frac{e^{-\lambda.\tau}}{\lambda} - \frac{1}{\lambda}\right]$$

$$Q(t) = 1 - \frac{1}{\lambda.\tau}.\left(1-e^{-\lambda.\tau}\right)$$

$$Q(t) = 1 - \frac{(1-e^{-\lambda.\tau})}{\lambda.\tau} \tag{4.19}$$

Outra fonte consultada (Isograph®, 1999) mostra uma forma alternativa para determinar a indisponibilidade média associada a bens no estado "*dormant*". Aqui, parte-se da seguinte expressão:

$$Q(t) = \frac{\lambda.\tau - (1-e^{-\lambda.\tau}) + \lambda.\tau_R.(1-e^{-\lambda.\tau})}{\lambda.\tau + \lambda.\tau_R.(1-e^{-\lambda.\tau})} \tag{4.20}$$

Voltando a assumir que o tempo médio de reparação (τ_R) se pode de certa forma ignorar, uma vez que tem pouca expressão comparativamente ao intervalo de tempo entre testes ou inspecções (τ) e que para o tipo de equipamentos estudados a questão da reparação de componentes aquando de uma solicitação não tem muito sentido, a expressão anterior simplifica-se, resultando:

$$Q(t) = \frac{\lambda.\tau - (1-e^{-\lambda.\tau})}{\lambda.\tau}$$

$$Q(t) = 1 - \frac{(1 - e^{-\lambda.\tau})}{\lambda.\tau} \qquad (4.21)$$

Assim, partindo dos pressupostos assumidos anteriormente[13], chegamos novamente à mesma expressão que em (4.19).

Hauptmanns *et al* (2008b) também utilizam uma expressão similar para determinar a indisponibilidade média de um sistema automático de extinção de incêndio. Zio (2007) apresenta um estudo mais completo sobre este tema, englobando outras situações além das falhas ocultas. Para tal, considera-se um bem que se encontra operacional no início da missão, podendo o seu ciclo de vida ser representado de acordo com a Figura 4.6.

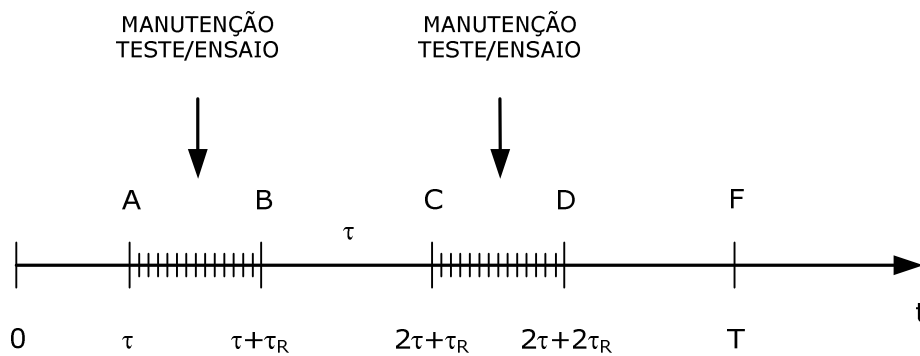



Figura 4.6 – Comportamento no tempo de um bem sujeito a manutenção, teste ou ensaio periódicos

Onde:

$\overline{OA}$ = Período de operação compreendido até à primeira intervenção (teste, ensaio, manutenção). A probabilidade de avaria do bem num tempo genérico "*t*" deve-se ao facto de:

- Ser solicitado em "*t*", mas encontrar-se em falha (com probabilidade Q_0);
- Ocorrência de falha aleatória oculta antes de "*t*" [$F(t)$].

Assim, a indisponibilidade instantânea em "*t*" ($0<t<\tau$), virá:

[13] De referir que se fosse assumido outro tipo de distribuição diferente da exponencial negativa, com função de risco não constante, a abordagem a esta questão levaria à apresentação de outras expressões matemáticas.

$$q_{OA}(t) = Q_0 + (1 - Q_0).F(t) \tag{4.22}$$

E o respectivo tempo médio inoperacional (*downtime*):

$$\overline{T}_{D(OA)} = \int_0^{\tau} q_{OA}(t).dt \tag{4.23}$$

$$\overline{T}_{D(OA)} = Q_0.\tau + (1 - Q_0).\int_0^{\tau} F(t).dt \tag{4.24}$$

$\overline{AB}$ = Período relativo ao teste, ensaio ou manutenção. O bem não se encontra operacional, sendo o tempo médio de inoperacionalidade (*downtime*) correspondente ao tempo dispendido em manutenção, teste ou ensaio:

$$\overline{T}_{D(AB)} = \tau_R \tag{4.25}$$

$\overline{BC}$ = Num tempo genérico "t_1" entre duas manutenções, o bem pode-se encontrar avariado devido a um erro ocorrido na anterior acção de manutenção (teste ou ensaio) (γ_0), ou como anteriormente, devido a uma falha quando solicitado (Q_0) ou a uma avaria aleatória antes de "t_1" [$F(t)$]. A indisponibilidade instantânea será dada por:

$$q_{BC}(t) = \gamma_0 + (1 - \gamma_0).\left[Q_0 + (1 - Q_0).F(t)\right] \tag{4.26}$$

Sendo o correspondente tempo médio de inoperacionalidade (*downtime*) dado por:

$$\overline{T}_{D(BC)} = \int_0^{\tau} q_{BC}(t).dt \tag{4.27}$$

$$\overline{T}_{D(BC)} = \gamma_0.\tau + (1 - \gamma_0).\left[Q_0.\tau + (1 - Q_0).\int_0^{\tau} F(t).dt\right] \tag{4.28}$$

$\overline{CF}$ = O ciclo normal de manutenção é repetido durante a vida "T" do bem. O número de ciclos de manutenção ($\overline{AB} - \overline{BC}$) é calculado através da seguinte expressão:

$$k = \frac{T}{\tau + \tau_R} \tag{4.29}$$

Desta forma podemos determinar o tempo médio de inoperacionalidade (*downtime*) até “*T*” através de:

$$\overline{T}_{D(OT)} = Q_0 + (1-Q_0).\int_0^\tau F(t).dt + \frac{T}{\tau+\tau_R}.\left\{\tau_R + \gamma_0.\tau + (1-\gamma_0).\left[Q_0.\tau + (1-Q_0).\int_0^\tau F(t).dt\right]\right\}$$

(4.30)

A indisponibilidade média virá:

$$Q_{0T} = \frac{\overline{T}_{D(0T)}}{T} \qquad (4.31)$$

$$Q_{OT} = \frac{Q_0}{T} + \frac{1-Q_0}{T}.\int_0^\tau F(t).dt + \frac{1}{\tau+\tau_R}.\left\{\tau_R + \gamma_0.\tau + (1-\gamma_0).\left[Q_0.\tau + (1-Q_0).\int_0^\tau F(t).dt\right]\right\}$$

(4.32)

Excluindo o período de tempo até à primeira manutenção, por a sua dimensão ser tipicamente muito inferior a “*T*”, ficamos com:

$$\overline{T}_{D(AF)} = \frac{T}{\tau+\tau_R}.\left\{\tau_R + \gamma_0.\tau + (1-\gamma_0).\left[Q_0.\tau + (1-Q_0).\int_0^\tau F(t).dt\right]\right\} \qquad (4.33)$$

Correspondendo uma indisponibilidade média:

$$Q_{OT} \cong \frac{\tau_R}{\tau} + \gamma_0 + (1-\gamma_0).\left[Q_0 + \frac{1-Q_0}{\tau}.\int_0^\tau F(t).dt\right] \qquad (4.34)$$

Se considerarmos um bem com avarias aleatórias, seguindo a lei exponencial, com taxa de avarias constante, a sua probabilidade de falha pode ser determinada através da expressão (4.35):

$$F(t) = 1 - e^{-\lambda.t} \qquad (4.35)$$

A indisponibilidade média pode ser determinada através da seguinte expressão:

$$Q_{OT} \cong \frac{\tau_R}{\tau} + \gamma_0 + (1-\gamma_0).\left[Q_0 + \left(\frac{1-Q_0}{\tau}\right).\left(\tau - \frac{1-e^{-\lambda.\tau}}{\lambda}\right)\right] \quad (4.36)$$

Na prática, a expressão anterior poderá ser simplificada, dado que γ_0<<1 e Q_0<<1:

$$Q_{OT} \cong \frac{\tau_R}{\tau} + \gamma_0 + Q_0 + \frac{1}{\tau}.\left(\tau - \frac{1-e^{-\lambda.\tau}}{\lambda}\right) \quad (4.37)$$

$$Q_{OT} \cong \frac{\tau_R}{\tau} + \gamma_0 + Q_0 + \left(1 - \frac{1-e^{-\lambda.\tau}}{\lambda.\tau}\right) \quad (4.38)$$

Na expressão anterior podem-se distinguir os vários contribuintes na indisponibilidade dos bens, nomeadamente:

$\frac{\tau_R}{\tau}$	Indisponibilidade durante a manutenção, teste ou ensaio
γ_0	Indisponibilidade devido a erro após intervenção
Q_0	Indisponibilidade devido a falha aquando da solicitação
$1 - \frac{1-e^{-\lambda.\tau}}{\lambda.\tau}$	Indisponibilidade devido a falhas aleatórias ocultas (entre testes)

De acordo com as razões anteriormente apresentadas, para o presente estudo são considerados irrelevantes os três primeiros tipos de indisponibilidade, considerando-se assim apenas as falhas aleatórias ocultas entre testes, determinando-se a indisponibilidade dos bens no estado "*dormant*" de acordo com a expressão simplificada (4.39), que coincide com as expressões (4.19) e (4.21).

$$Q_{OT} \cong \left(1 - \frac{1-e^{-\lambda.\tau}}{\lambda.\tau}\right) \quad (4.39)$$

Será esta a expressão utilizada para o cálculo da indisponibilidade de um bem no estado "*dormant*", para uma dada taxa de avarias constante específica deste estado (λ) e com um determinado intervalo de tempo entre testes, ensaios ou inspecções (τ).

4.5.2 – Exemplo de aplicação

Para exemplificar de uma forma simples a aplicação desta teoria recorre-se a um exemplo envolvendo um detector de incêndios (Rausand & Hoyland, 2004). De acordo com a base de dados OREDA (2002) a taxa de avarias para um tipo específico de detector de incêndios é λ=0,21x10^{-6} avarias por hora.

Se esta unidade for testada trimestralmente (aprox. 2190 horas), obtem-se o valor referente à sua indisponibilidade, utilizando a expressão (4.39).

$$Q(t) = \left(1 - \frac{1 - e^{-0,21x10^{-6}.2190}}{0,21x10^{-6}.2190} \right) = 0,0002298 \cong 2,298x10^{-4}$$

Utilizando a expressão simplificada (4.17), obter-se-ia:

$$Q(t) \cong \frac{0,21x10^{-6}.2190}{2} = 0,0002299 \cong 2,300x10^{-4}$$

A primeira conclusão que se pode tirar é de que utilizando a expressão simplificada (4.17) se obtêm sempre valores conservativos, ligeiramente superiores aos valores correctos calculados através da expressão (4.39).

Outra leitura que se pode tirar do cálculo efectuado é de que, na eventualidade de ocorrência de um incêndio, a probabilidade média do detector não funcionar é de aproximadamente 0,00023, o que significa uma falha em cada 4350 incêndios.

Outra forma de ler o resultado obtido é afirmar que o referido detector não se encontra disponível em cerca de 0,023% do tempo, correspondendo a aproximadamente 2 horas por ano, se o mesmo for considerado em operação contínua durante esse período.

Sistema Paralelo

Se a análise incidir agora sobre dois detectores de incêndio idênticos (igual taxa de avarias, ensaiados ao mesmo tempo com um período entre testes "τ"), e se assumir que apenas é necessário que um dos dois detectores funcione para que o sistema cumpra a sua função, a indisponibilidade do sistema pode ser determinada na sua forma simplificada pela expressão (4.40), resultante de (4.7).

$$Q(\tau) = 1 - \frac{\int_0^{\tau} R(t).dt}{\tau} \qquad (4.40)$$

Como a fiabilidade de um sistema paralelo com uma redundância é dada por:

$$R(t) = 2e^{-\lambda.t} - e^{-2\lambda.t} \qquad (4.41)$$

Logo:

$$Q(\tau) = 1 - \frac{2}{\lambda.\tau}.(1 - e^{-\lambda.\tau}) + \frac{1}{2.\lambda.\tau}.(1 - e^{-2.\lambda.\tau}) \qquad (4.42)$$

Substituindo $e^{-\lambda.t}$ pela sua série de Maclaurin, e assumindo que $(\lambda.\tau)$ é pequeno, poder-se-á fazer a seguinte aproximação[14]:

$$Q(\tau) \cong \frac{1}{3}.(\lambda.\tau)^2 \qquad (4.43)$$

Desta forma, utilizando os mesmo valores do exemplo anterior obtem-se uma indisponibilidade média para o sistema paralelo de:

$$Q(\tau) \cong \frac{1}{3}.(0{,}21x10^{-6}x2190)^2 \cong 7{,}1x10^{-8}$$

Significando uma probabilidade de falha do sistema quando solicitado (PFOD) muito baixa, ou uma alta disponibilidade, comparativamente à calculada para um "sistema" composto por um único detector.

---

[14] Uma vez que a indisponibilidade de um componente isolado é dada pela expressão (4.17), seria de esperar que a indisponibilidade do sistema paralelo de dois componentes fosse dada por $(\lambda.\tau/2)^2 = (\lambda.\tau)^2/4$, ao contrário da expressão (4.43) que é a correcta. Tal diferença deve-se ao facto de a média de um produto não ser igual ao produto das médias. Neste caso, a não utilização da expressão (4.43) levaria a um resultado não conservador.

Sistema Paralelo Restrito (k/n)

Para um sistema paralelo restrito "2 em 3", e assumindo os pressupostos anteriores, a indisponibilidade do sistema é dada por:

$$Q(\tau) \cong (\lambda.\tau)^2 \tag{4.44}$$

Assim, a indisponibilidade do sistema de detectores de incêndio, onde pelo menos dois dos detectores são necessários para o sistema ter sucesso, terá o seguinte valor:

$$Q(\tau) \cong (0{,}21x10^{-6}\,x2190)^2 \cong 2{,}1x10^{-7}$$

Sistema Série

Por fim, para um sistema série de dois detectores de incêndio independentes, e voltando a assumir-se os mesmos pressupostos, poder-se-á determinar a indisponibilidade do sistema através da expressão (4.45).

$$Q(\tau) \cong \frac{(\lambda_1 + \lambda_2).\tau}{2} = \frac{\lambda_1.\tau}{2} + \frac{\lambda_2.\tau}{2} \tag{4.45}$$

O que significa que a indisponibilidade de um sistema série pode ser determinada através da soma das indisponibilidades dos seus componentes individualmente.

4.6 – Probabilidade de ocorrência de uma situação crítica

Para se determinar a probabilidade de ocorrência de uma situação crítica ter-se-á inicialmente que definir um acontecimento acidental e a barreira de segurança existente para fazer face a esse acontecimento. Assume-se que o acontecimento acidental (ex. fogo) ocorre de forma aleatória de acordo com um Processo Homogéneo de Poisson (HPP), com uma intensidade[15] "ϕ" (Rausand & Hoyland, 2004).

[15] Para evitar algumas confusões não se refere este parâmetro como "taxa de avarias". O autor refere o termo "intensidade", que no contexto específico corresponde ao número médio de acontecimentos por unidade de tempo, denominando-se também em alguma literatura por taxa de solicitação do processo (*process demand rate*).

Desta forma, uma situação crítica ocorre quando se dá o acontecimento acidental e a barreira de segurança se encontra indisponível. Neste momento assume-se que a indisponibilidade se encontra associada apenas à existência de falhas ocultas.

De acordo com o descrito no **Anexo I**, nomeadamente sobre a Distribuição de Poisson (A1.6), substituindo a taxa média de ocorrência do insucesso (μ) pelo produto da intensidade (ϕ) pela indisponibilidade da barreira de segurança (Q(t)), obtem-se a probabilidade de obter "n" situações críticas "*Nc(t)*" através da expressão (4.46).

$$\Pr\left[Nc(t)=n\right]=\frac{\left[\phi.Q(t).t\right]^{n}}{n!}.e^{-\phi.Q(t).t} \qquad para\ n=o,1,... \tag{4.46}$$

Sendo o número médio de situações críticas no intervalo [0,t], dado por:

$$\overline{Nc}(t)=\phi.Q(t).t \tag{4.47}$$

Referindo como exemplo o caso do detector de incêndio descrito no parágrafo 4.5.2, e assumindo que em média ocorrem 7,64x10^{-4} incêndios por hora para o tipo de edifício, dimensão ou situação particular (Lin, 2005), pode-se determinar a probabilidade de ocorrer 1 (uma) situação crítica em cada período de tempo entre testes ou ensaios (trimestre):

$$\Pr\left[Nc(t)=1\right]=\frac{\left[7{,}64x10^{-4}\,x2{,}30x10^{-4}\,x2190\right]^{1}}{1!}.e^{-7{,}64x10^{-4}x2{,}30x10^{-4}x2190}=3{,}85x10^{-4}$$

Correspondendo assim a uma probabilidade de cerca de 0,04%. Ainda de acordo com a expressão (4.47) ocorrerão por ano uma média de 0,0015 situações críticas, ou seja, simultaneidade de um acontecimento acidental (incêndio) e indisponibilidade da barreira de segurança.

4.7 – Conclusões do Capítulo

No presente capítulo pretendeu-se mostrar as particularidades inerentes aos bens que se encontram no estado "*dormant*", começando especificamente por definir os vários

estados em que os equipamentos se podem encontrar do ponto de vista funcional, assim como algumas razões que levam a uma determinada condição.

Para os bens que não se encontram em operação, clarificaram-se as diferenças entre o que se entende por um bem em armazém (“*storage*”), um bem em “*standby*” e um bem no estado “*dormant*”, tendo sido referidos alguns trabalhos que abordam cada um dos casos.

As barreiras de segurança podem ser consideradas bens no estado “*dormant*”, uma vez que passam a maior parte do seu ciclo de vida neste estado (embora experimentem outros em determinados períodos). Para este tipo de equipamentos, pretende-se que os mesmos funcionem cada vez que forem solicitados, ou seja, que estejam disponíveis. Complementarmente, deseja-se que após a solicitação haja um período, ou missão, durante o qual o sistema funcione sem falhas (fiabilidade). Qualquer falha (considerada potencialmente perigosa) que ocorra em cada uma das fases anteriormente referidas porá em causa todo o sistema, inibindo a barreira de segurança de cumprir a função para a qual foi projectada e instalada.

Para bens no estado “dormant”, as potenciais falhas ocultas (*hidden failures*) só serão conhecidas aquando de uma solicitação real ou durante testes e ensaios. Assim, a periodicidade com que esses testes ou ensaios são efectuados mostra-se um factor de grande importância no propósito de identificar as falhas ocultas, e consequente probabilidade de falha quando solicitado (PFOD), ou simplesmente a sua indisponibilidade.

Foram apresentadas algumas metodologias de análise, assim como algum criticismo relativamente a alguns pressupostos assumidos nessas metodologias.

Mostrou-se a importância da diferenciação entre os componentes considerados de suporte (ou arranque) e os componentes activos, uma vez que para este tipo de barreiras de segurança cada tipo de componente terá a sua intervenção em cada fase distinta.

Apresentaram-se algumas expressões matemáticas que permitem determinar a indisponibilidade de uma barreira de segurança, tendo por base as falhas ocultas dos seus componentes. Finalizou-se o capítulo com alguns exemplos de aplicação prática e sua interpretação.

CAPÍTULO V

METODOLOGIA PROPOSTA

5.1 – Introdução

Hoje em dia as análises de fiabilidade, manutibilidade, disponibilidade e segurança tornaram-se uma parte integrante do projecto de sistemas, especialmente quando se trata de aplicações críticas. Os sistemas projectados são cada vez mais complexos e maiores e os seus componentes exibem comportamentos e interacções cada vez mais difíceis de analisar e modelar (Boudali & Dugan, 2005).

Tendo em atenção a importância da temática da segurança contra incêndios, e o exposto nos capítulos anteriores referentes ao risco, risco de incêndio, metodologias de análise e singularidade do tipo de equipamentos designados por barreiras de segurança, pretende-se criar um modelo que permita determinar a probabilidade de falha (ou sucesso) para os equipamentos tipo "*dormant*", uma vez que se trata de uma questão não tão explorada em termos científicos, mas que em instalações industriais de alto risco assume um papel fundamental em matéria de segurança.

Com a metodologia desenvolvida, adiante designada por "***Metodologia RODS***" (***R****eliability* ***O****f* ***D****ormant* ***S****ystems*), pretende-se explorar este tipo particular de equipamentos, cujo trabalho passa pelo desenvolvimento de uma metodologia em termos teóricos, mas tendo sempre em vista a sua aplicação prática em sistemas reais. O objectivo da Metodologia RODS será o de encontrar valores para cada barreira de segurança que conduzam ao conhecimento da probabilidade de sucesso da mesma, e assim saber qual a probabilidade de se poder evitar um acontecimento indesejado.

Como é do conhecimento geral, os equipamentos ou sistemas que se encontram no estado "*dormant*" são muitas vezes esquecidos no que se refere a acções de manutenção preventiva ou realização de testes periódicos destinados a aferir a sua operacionalidade. Pretende-se assim modelar o cálculo da fiabilidade das barreiras de segurança contra incêndios, tendo como objectivo a sua eventual aplicação futura neste tipo de bens que normalmente se encontram instalados em praticamente todas as instalações industriais consideradas de risco elevado. A Figura 5.1 serve para mostrar como a gestão deste tipo de barreira de segurança pode influenciar um dos elementos a considerar, nomeadamente no que se refere à mitigação ou diminuição da gravidade das consequências, e assim directamente no risco de incêndio.

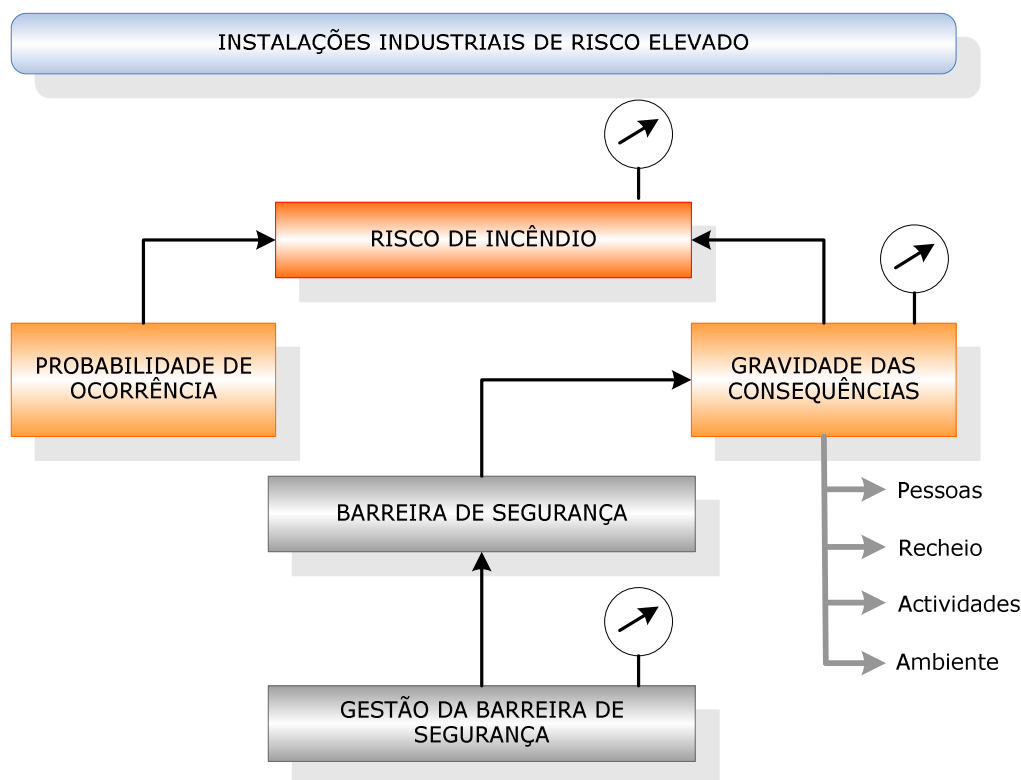



Figura 5.1 – Influência da gestão das barreiras de segurança no risco de incêndio

Com a aplicação da metodologia pretende-se conhecer a fiabilidade da barreira de segurança, e consequentemente o grau de protecção das instalações, que em conjunto com as complementares medidas de prevenção[16], contribuam para se alcançar um nível de risco na instalação que se possa considerar tolerável ou aceitável.

[16] De acordo com a descrição efectuada no Capítulo III, as medidas de prevenção visam reduzir a probabilidade de ocorrência de incêndio

5.2 – Metodologia RODS

Tal como referido no capítulo anterior, assume-se que as duas fases em estudo, nomeadamente a análise da disponibilidade quando solicitado e a fiabilidade em serviço, são teoricamente independentes até determinado momento. Para justificar esta afirmação, clarifica-se de seguida o conceito de independência para qualquer que seja o tipo de barreira de segurança em estudo. Como é óbvio, o equipamento permanece o mesmo, com os mesmos subsistemas e componentes e existe uma clara relação em termos funcionais entre as duas fases, uma vez que uma falha do equipamento na primeira fase inibe qualquer expectativa de sucesso referente à segunda.

No entanto, como os dois tipos de análise incidem sobre aspectos e estados diferentes do funcionamento do equipamento, com modos de falha em alguns casos distintos e valores dos parâmetros em análise por vezes bastante diferentes, a lógica subjacente ao tratamento da fiabilidade global das barreiras de segurança justifica a independência no tratamento das fases. No cálculo da fiabilidade global assume-se que o insucesso de qualquer uma das fases provoca a falha da barreira de segurança.

Assim, de acordo com o enquadramento efectuado para esta temática, e de uma forma simplificada, a Metodologia RODS pode à partida ser descrita como uma análise que é efectuada tendo em conta as duas fases, embora neste estudo se tenha dado grande relevo à primeira fase, uma vez que é reconhecida a elevada importância e influência da fase de arranque das barreiras de segurança quando solicitadas.

Grande parte dos problemas surge precisamente aquando da solicitação dos equipamentos quando estes se encontram indisponíveis, e não durante o período ou missão em que se encontram a funcionar em regime estável. Normalmente, após a fase de arranque, não surgem problemas associados ao funcionamento da barreira de segurança.

A Metodologia RODS pode ser representada de uma forma esquemática conforme se mostra na Figura 5.2.

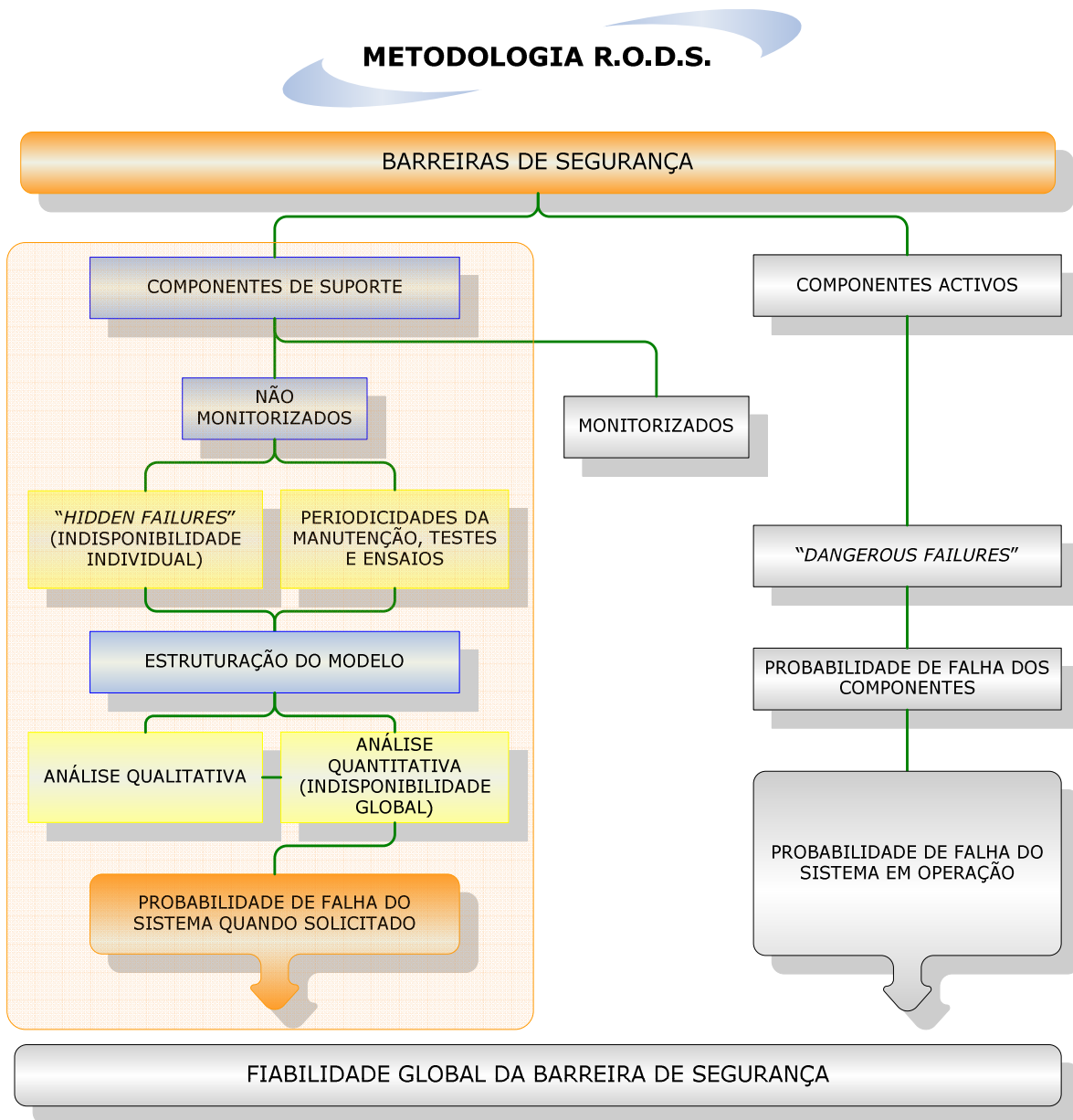



Figura 5.2 – Metodologia RODS *(Reliability Of Dormant Systems)*

Desta forma, o desenvolvimento do trabalho será dedicado à determinação da probabilidade de transição do sistema do estado "*dormant*" para o estado de operação, focalizando a disponibilidade da barreira quando esta é solicitada, correspondendo à zona sombreada da Figura 5.2, adiante designada por "primeira fase".

De acordo com o esquema apresentado, a primeira fase da Metodologia RODS engloba as seguintes tarefas:

1. Definição da barreira de segurança
   - 1.1. Descrição do comportamento da barreira de segurança, quando solicitada;
   - 1.2. Identificação dos componentes de suporte (ou arranque);
   - 1.3. Identificação dos componentes de suporte não monitorizados;
   - 1.4. Identificação dos modos de falha ou acontecimentos relativos aos componentes de suporte não monitorizados;
   - 1.5 Definição das periodicidades referentes às actividades de Manutenção, testes ou ensaios da barreira de segurança.
2. Construção de uma Árvore de Falhas
   - 2.1. Análise qualitativa da Árvore de Falhas;
   - 2.2. Análise quantitativa da Árvore de Falhas.

5.2.1 - Descrição detalhada da primeira fase da Metodologia RODS

Os próximos parágrafos visam descrever de uma forma mais detalhada a primeira fase da metodologia proposta (Metodologia RODS), explicando as várias etapas, assim como referenciar as ferramentas fiabilísticas utilizadas em cada uma delas. De forma a se compreender melhor algumas dessas ferramentas, oportunamente serão apresentadas as suas particularidades e referências de suporte.

5.2.1.1 – Definição da barreira de segurança

No início do estudo deverá realizar-se uma descrição do equipamento em análise, definido como barreira de segurança. Deverá ser descrita a sua função, os seus sistemas, subsistemas, unidades e componentes, fronteiras do sistema, data de início de funcionamento e parâmetros de funcionamento, assim como as normas de construção (e instalação) seguidas e toda a informação que se possa considerar relevante e que contribua para a completa caracterização da barreira de segurança. É aconselhável que o documento descritivo da barreira de segurança seja acompanhado e complementado por esquemas ou diagramas tipo P&I e desenhos da instalação. A informação constante neste documento não irá fazer parte dos cálculos que servirão para determinar a probabilidade de falha da barreira de segurança quando solicitada, mas permitirá conhecer melhor o equipamento e as suas características principais, fazendo parte integrante do processo relativo ao estudo da fiabilidade da barreira de segurança.

5.2.1.2 - Identificação dos componentes de suporte (ou de arranque)

De acordo com a Metodologia RODS proposta, representada esquematicamente na Figura 5.2, e no seguimento da primeira etapa anteriormente referida, é necessário identificar quais os componentes que têm uma intervenção especial na primeira fase, estando vigilantes enquanto o equipamento se encontra no estado "*dormant*", actuando no momento em que o mesmo é solicitado para entrar em serviço e cessando a sua função após essa entrada em funcionamento. Estes componentes designam-se de suporte ou arranque e, como são alvo de um estudo independente, é necessário que nesta fase não haja dúvidas na identificação dos mesmos.

5.2.1.3 - Identificação dos componentes de suporte monitorizados e não monitorizados

Entre os componentes designados de suporte, poderão existir alguns que se encontram monitorizados continuamente[17]. Embora esta situação fosse desejável para todos os componentes, razões de ordem física (ou funcional) e de ordem económica fazem com que tal não seja viável. Em alguns casos, neste tipo de sistemas, verifica-se até uma ausência quase total de componentes sujeitos a monitorização.

A existência de componentes de suporte monitorizados é bastante importante e deverá ser tida em conta, uma vez que para esses componentes uma avaria ocorrida num dado instante "*t*" é teoricamente conhecida de imediato, levando à tomada de acções de natureza correctiva, fora dos períodos normais de inspecção, teste ou ensaio.

Caso as avarias ocorram em componentes de suporte não monitorizados, só no momento em que se realizam ensaios ou testes periódicos teremos conhecimento da sua existência, designando-se por isso como falhas ocultas (*hidden failures*). A gravidade da ocorrência destas falhas aumenta quando as mesmas não são detectadas nos referidos

[17] A monitorização em contínuo pressupõe a transmissão e tratamento de sinais em tempo real. Mesmo que o equipamento principal se encontre numa zona não observada, a informação sobre o estado deste tipo de componentes é passível de ser conhecida através de um sistema de gestão técnica centralizada (G.T.C.) ou um quadro repetidor de sinais (Q.R.S.) que se encontre numa zona vigiada.

testes ou ensaios periódicos, mas apenas reveladas numa solicitação em situação real de acidente.

Na metodologia proposta, identificam-se os componentes que se encontram a ser monitorizados, assumindo-se que a eventual transmissão das falhas à distância se encontra efectuada nas devidas condições e que existe vigilância 24/24 horas para actuar em conformidade. Trata-se de um cenário que não é por vezes real, tendo na prática também que ser equacionada a já referida fiabilidade humana, entre outros aspectos. No entanto, na Metodologia RODS parte-se do pressuposto que apenas os componentes não monitorizados podem possuir as designadas potenciais falhas ocultas, sendo este tipo de componentes alvo de análise fiabilistica.

De referir que existem alguns estudos sobre a detecção de falhas, apresentando o desenvolvimento de algumas metodologias e técnicas de análise. Bartlett et al (2009) afirmam que a funcionalidade de qualquer sistema ou a eficácia das missões é maximizada através de uma detecção das falhas o mais rápido que for possível, podendo-se assim alterar as missões, reconfigurar os sistemas e aprovisionar sobressalentes com maior celeridade. Para tal, mostram duas abordagens desenvolvidas sobre o diagnóstico de falhas com base em Árvore de Falhas e diagramas denominados "*digraphs*", que representam as inter-relações entre as variáveis do processo (ex. temperatura, caudal ou pressão). Nesta área, outros trabalhos podem ser analisados (Hurdle *et al*, 2007) (Iverson & Pattersine-Hine, 1995).

5.2.1.4 – Identificação das potenciais falhas dos componentes de suporte

Nesta fase encontra-se inserida a análise aos componentes de suporte não monitorizados, adiante designados apenas como componentes de suporte. Como se trata de uma etapa do estudo bastante importante, é necessário apresentar algumas bases que fundamentam as opções assumidas.

Pressupostos:

1. O sistema é composto por componentes não-reparáveis, e não é possível proceder-se à sua substituição, uma vez solicitados;
2. Embora possa ser discutível, após cada inspecção, teste e ensaio, o sistema é considerado AGAN (*as good as new*);
3. Os tempos até à avaria dos componentes seguem uma distribuição exponencial;

4. No cálculo da indisponibilidade, considera-se o tempo "*t*" como o período "*dormant*";
5. No cálculo da indisponibilidade, considera-se o tempo "τ" como o período entre testes/ensaios;
6. O tempo relativo às inspecções, testes ou ensaios periódicos é considerado negligenciável no presente estudo;
7. O tempo relativo às acções de manutenção correctiva (quer as referentes aos componentes monitorizados, quer as detectadas aquando das inspecções, testes e ensaios) também é considerado negligenciável.

Depois de identificados os componentes de suporte não monitorizados, há que estudar bem o seu comportamento e determinar os potenciais acontecimentos relacionados com modos de falha que poderão ocorrer, e que podem pôr em causa o arranque do equipamento quando solicitado.

Desta forma, é elaborada uma listagem dos acontecimentos potencialmente perigosos que levam à falha dos componentes seleccionados, apresentando-se também a indisponibilidade relacionada com esses componentes e modos de falha, quando os mesmos se encontram no estado "*dormant*".

5.2.1.5 – Estruturação do modelo

De acordo com a identificação dos potenciais acontecimentos relativos aos componentes de suporte seleccionados anteriormente, recorre-se a uma técnica gráfica, a Árvore de Falhas, cuja descrição já foi alvo de apresentação no ponto 2.3.10.4. Nesta construção, é colocada como falha principal, ou evento de topo, a falha no arranque do sistema ou barreira de segurança, analisando-se de seguida todos os acontecimentos subsequentes que a podem originar. Esta lógica dedutiva repetir-se-á até se alcançarem os denominados acontecimentos básicos em consideração, tendo em conta os arranjos funcionais entre os mesmos através da utilização das portas lógicas, também referido no Capítulo II.

Na construção da Árvore de Falhas deve-se ter bastante atenção às interdependências, ou dependências funcionais, entre os acontecimentos, uma vez que o reconhecimento de tais situações condicionará o resultado final.

Desta forma serão bem identificadas as situações denominadas sub-Árvores dinâmicas (relacionadas com as interdependências e sequências funcionais) e as sub-Árvores estáticas (acontecimentos independentes), sendo posteriormente analisados de forma distinta por Análises de Markov ou por técnicas combinatórias normalizadas (que consideram a probabilidade dos acontecimentos e as portas lógicas indicadas) como os Diagramas de Decisão Binária (BDD), respectivamente.

Este tema das dependências funcionais é de facto fulcral. De acordo com Zio (2009), todos os sistemas tecnológicos modernos são altamente redundantes mas continuam a avariar devido às avarias dependentes. O mesmo autor afirma que a modelação deste tipo de avarias continua a ser um assunto crítico na Avaliação Probabilistica de Segurança (PSA – *Probabilistic Safety Assessment*), uma vez que as avarias dependentes podem provocar a falha de barreiras de segurança, contribuindo significativamente para o risco. A quantificação dessa contribuição é assim necessária para evitar subestimar grosseiramente o risco.

Algumas estratégias gerais para evitar avarias dependentes são (Zio, 2009):

- Barreiras – Impedimentos físicos para confinar ou restringir a condição potencialmente perigosa;
- Formação – Treinar o pessoal para assegurar que os procedimentos são seguidos em todas as condições de operação;
- Controlo de qualidade – Assegurar que o produto está conforme com o projecto e a sua operação e manutenção seguem os procedimentos e normas aprovados;
- Redundâncias;
- Manutenção preventiva;
- Monitorizar, testar e inspeccionar;
- Diversificar – Diversificar fabricantes, aspectos funcionais e princípios de operação.

5.2.1.6 – Análise qualitativa da Árvore de Falhas

Tal como referido no Capítulo II, a análise qualitativa de uma Árvore de Falhas tem como objectivo determinar os conjuntos de corte mínimos (MCS - *minimal cut sets*). Com base nestes conjuntos são determinadas todas as combinações de acontecimentos que levam à falha principal.

Alguns trabalhos analisados (Andrews & Moss, 2002) apresentam também uma abordagem pela positiva, determinado o conjunto de caminhos mínimos (MPS – *minimal path sets*) que levam ao sucesso de um sistema. Obviamente que qualquer uma das duas abordagens levará a resultados complementares.

No entanto, de acordo com a complexidade dos sistemas em análise, verifica-se que em alguns casos se obtém um grande número de conjuntos mínimos (caminhos ou corte), cujo cálculo da probabilidade das combinações possíveis se torna impraticável na fase posterior de quantificação da Árvore de Falhas.

Quando se utiliza o MCS, e se tem em conta apenas os primeiros termos (termos de primeira, de segunda e eventualmente de terceira ordem), alcançamos uma aproximação bastante razoável da probabilidade de falha do sistema, o que não se verifica quando utilizamos o MPS. Por esta razão, a quantificação é normalmente realizada utilizando o conjunto de cortes mínimo (MCS).

A análise qualitativa pode ser efectuada manualmente através de uma abordagem "*top-down*" ou "*bottom-up*" utilizando as operações booleanas e os métodos de substituição, expansão e redução (Andrews & Moss, 2002). Obviamente que quando se trata de Árvores de Falhas com alguma complexidade e dimensão ter-se-á que recorrer a programas informáticos. No caso da Árvore de Falhas que não possuem acontecimentos mutuamente exclusivos pode-se utilizar o já referido algoritmo MOCUS[18].

Após a realização da análise qualitativa, fica-se com um conjunto de informações que permitem olhar para os acontecimentos básicos que compõem a Árvore de Falhas e verificar qual, ou quais, são responsáveis pela ocorrência do acontecimento de topo, e em que escala de importância, tendo em conta a conjunção de acontecimentos.

5.2.1.7 – Análise quantitativa da Árvore de Falhas

É neste ponto que finalmente se determina o valor referente à probabilidade de falha do sistema quando solicitado (PFOD), correspondendo esse resultado ao objectivo principal subjacente à primeira fase da Metodologia RODS. Para tal, aproveita-se o trabalho realizado na etapa anterior, utilizando os conjuntos de corte mínimos da análise

[18] "*Method Of Obtaining Cut Sets*" – Ver Capítulo II

qualitativa da Árvore de Falhas, quando assumidamente os acontecimentos são independentes.

Para a análise quantitativa é fundamental conhecerem-se determinados valores, tais como as periodicidades com que as acções de Manutenção (nomeadamente os testes ou ensaios) são efectuadas e as taxas de avaria referentes aos acontecimentos básicos. Esta é uma das maiores dificuldades encontradas quando se pretende partir para uma análise fiabilística de equipamentos no estado "*dormant*". Normalmente não se conhecem, e praticamente não existe informação ou bases de dados com indicações sobre taxas de avarias para os bens que se encontram neste estado específico. No entanto, para se realizar uma análise quantitativa, o conhecimento deste parâmetro é fundamental para o cálculo da indisponibilidade média, tal como visto no capítulo anterior.

Na Metodologia RODS, e na impossibilidade de se seguir uma base de dados existente como por exemplo a OREDA[19], a taxa de avarias é normalmente determinada em função da informação de fabricantes dos equipamentos, uma vez que basicamente são estas as únicas entidades que possuem este tipo de informação, e em alguns casos apenas baseada na experiência.

Como a duração do tempo de vida em análise para este tipo de bens é relativamente grande, ou a idade dos mesmos é por vezes desconhecida, e assumindo que o sistema se encontra bem mantido através de rotinas estabelecidas, é normal considerar-se que os bens atingiram um comportamento estabilizado ou regime estacionário (*steady-state behavior*). Desta forma, o método de análise escolhido, usando a expressão (4.39) é o mais indicado, sendo referido em alguma bibliografia como "*Lambda Tau Analysis Method*", precisamente porque são estes dois parâmetros (λ,τ) que são utilizados para determinar a indisponibilidade dos bens em causa.

Quando existem acontecimentos dependentes, tal como referido no Capítulo II, ter-se-á que isolar as sub-Árvores respectivas, denominadas dinâmicas, e fazer uma análise com recurso a Cadeias de Markov (transições entre estados), onde essas dependências já podem ser representadas. No fim integram-se os resultados obtidos nas diversas sub-Árvores, quer as estáticas, quer as dinâmicas.

---

[19] Referido em 2.3.6

5.2.1.8 – Outras informações relevantes na análise da Árvore de Falhas

Após a análise quantitativa da Árvore de Falhas é possível obter outras informações de relevo, nomeadamente obter dados que permitam conhecer as medidas de importância (*Importance Measures*) referentes a cada acontecimento básico da Árvore de Falhas que se encontra relacionado com um determinado modo de falha, de modo a introduzir melhorias da forma mais eficaz e adequada. Estas medidas de importância são referidas muitas vezes como uma análise de sensibilidade (*Sensitivity Analysis*) (Ou & Dugan, 2000) (Assaf & Dugan, 2004).

As medidas de importância são utilizadas para detectar pontos fracos do projecto e modos de falha críticos do ponto de vista funcional do sistema. Permitem identificar o(s) acontecimento(s) da Árvore de Falhas cuja melhoria terá maior reflexo no desempenho do sistema.

As três medidas de importância mais frequentemente utilizadas são:

- *Birnbaum* – Determina o aumento máximo no risco quando um componente "X" se encontra em falha, quando comparado com a situação em que o mesmo se encontra a funcionar;
- *Criticality* – Dada a ocorrência do acontecimento de topo, determina a probabilidade da falha estar relacionada com a avaria de um componente "X";
- *Fussell-Vesely* – Dada a falha do sistema, determina a probabilidade com que o componente "X" tenha contribuído para a mesma ocorrência.

A escolha para a utilização de um dos métodos anteriores é importante, tendo em vista o objectivo a alcançar. Assim:

- Se for possível diminuir a indisponibilidade de cada acontecimento na mesma quantidade e com o mesmo esforço, dever-se-ão utilizar as medidas de importância *Birnbaum*;
- Se as melhorias apenas podem ser efectuadas em acontecimentos que possuam altas indisponibilidades, ou se o objectivo é dar prioridade aos esforços da manutenção, dever-se-ão utilizar as medidas de importância de criticidade ou criticalidade (*Criticality*);
- Se o objectivo é minimizar as contribuições individuais dos acontecimentos básicos, dever-se-ão utilizar as medidas de importância *Fussel-Vesely*;

Vejamos alguns aspectos particulares de cada uma das três metodologias acima referidas, designadas como principais.

Birnbaum – A medida de importância é dada por:

$$I_B(A) = P\{X \mid A\} - P\{X \mid \sim A\} \tag{5.1}$$

Onde "*A*" indica o acontecimento cuja importância está a ser medida, "*X*" indica o acontecimento de topo e "~*A*" a não ocorrência do acontecimento. Quando as indisponibilidades individuais dos acontecimentos não são conhecidas, o cálculo é determinado considerando uma indisponibilidade individual de 0,5.

Esta medida de importância é útil mas não considera a probabilidade de ocorrência do acontecimento, sendo independente do valor da indisponibilidade do mesmo, o que pode fazer com que se atribuam medidas de importância elevadas a acontecimentos pouco prováveis de ocorrer e que possam ser dificilmente melhorados. Desta forma, para focar apenas os acontecimentos críticos e de maior probabilidade de ocorrência, surge uma medida de importância *Birnbaum* modificada, designada de medida de importância de criticidade ou criticalidade (*Criticality*).

Criticality – Esta medida de importância é dada por:

$$I_C(A) = I_B(A).\frac{P\{A\}}{P\{X\}} = (P\{X \mid A\} - P\{X \mid \sim A\}.\frac{P\{A\}}{P\{X\}} \tag{5.2}$$

A medida de importância de criticidade ou criticalidade de um acontecimento "*A*" corresponde à probabilidade do componente "*A*" ser crítico para o sistema e que ocorreu sempre que o acontecimento de topo ocorre. Desta forma, esta medida considera além da probabilidade condicional (como a *Birnbaum*) também a probabilidade de ocorrência do acontecimento de topo devido ao acontecimento "*A*".

Esta medida de importância modifica a medida *Birnbaum* ajustando para a probabilidade relativa do acontecimento "*A*" de forma a reflectir a probabilidade de ocorrência do acontecimento e de que forma é possível melhorar o mesmo. Isto faz com que esta medida de importância se concentre nos acontecimentos básicos realmente importantes e seja possível comparar acontecimentos básicos entre Árvores de Falhas. A medida de

importância de criticidade ou criticalidade é apropriada quando se pretende a melhoria do desempenho do sistema.

Fussell-Vesely – Esta medida é utilizada em situações onde o acontecimento "*A*" contribui para o acontecimento de topo (significa pelo menos pertencer a um conjunto de cortes mínimo), embora não seja necessariamente um acontecimento crítico. Esta medida é o quociente entre a probabilidade de ocorrência de qualquer conjunto de corte que contenha o acontecimento "*A*" e a probabilidade de ocorrência do acontecimento de topo.

A medida de importância *Fussell-Vesely* é construída a partir dos conjuntos de cortes mínimos (MCS) e utiliza-se fundamentalmente quando o objectivo for minimizar as contribuições individuais dos acontecimentos básicos.

Além das metodologias anteriores existem outras medidas de importância probabilísticas que também podem ser referidas, tais como a medida *Fussell-Vesely* da importância do conjunto de cortes mínimo (*Fussell-Vesely measure of minimal cut set importance*), a medida *Barlow-Proschan* de importância do iniciador (*Barlow-Proschan measure of initiator importance*), a medida *Barlow-Proschan* da importância do conjunto de cortes mínimo (*Barlow-Proschan measure of minimal cut set importance*) e a medida contributória sequencial de importância activa (*Sequential contributory measure of enabler importance*) (Andrews & Moss, 2002).

Rausand e Hoyland (2004) referem complementarmente outras medidas de importância, como a medida potencial de melhoria (*The improvement potential measure*), importância ou valia do risco alcançado (*risk achievement worth*) e importância ou valia da redução do risco (*risk reduction worth*). Estes autores referem que a importância de um componente depende de dois factores, nomeadamente a localização do componente no sistema e a sua fiabilidade individual (tendo por vezes que se considerar a incerteza associada a essa fiabilidade).

5.3 – Conclusões do Capítulo

Neste capítulo é apresentada uma metodologia para análise de bens no estado "*dormant*", designada Metodologia RODS (*Reliability Of Dormant Systems*). O objectivo da metodologia apresentada é determinar a fiabilidade associada a uma determinada

barreira de segurança. O valor calculado servirá como indicador do maior ou menor sucesso quando ocorre um evento desta natureza, cujo resultado condicionará a gravidade ou severidade das consequências. Desta forma é apresentado um esquema com as diferentes fases da metodologia RODS.

A primeira fase da metodologia RODS incide sobre uma etapa fundamental e principal do funcionamento global destes tipo de barreiras, ou seja, a fase de arranque, e mais concretamente na probabilidade de sucesso na transição do estado "*dormant*" para o estado de operação activa. Desta forma, são apresentadas com algum detalhe as etapas que constituem a primeira fase, sendo esta a principal questão alvo de estudo no presente trabalho.

É dada particular importância aos designados componentes de suporte ou arranque que não se encontram monitorizados. São apresentados alguns pressupostos ou bases de partida para a aplicação da metodologia, bem como a indicação das principais dificuldades que sobressaem da aplicação da mesma.

É abordado com algum detalhe a construção da Árvore de Falhas, e especificadas as ferramentas utilizadas na análise qualitativa e quantitativa. São referidas outras características da metodologia RODS, como a possível interpretação de outras informações resultantes da análise quantitativa, designadas medidas de importância (*Importance Measures*) ou análise de sensibilidade (*Sensitivity Analysis*). Neste aspecto são detalhadas as medidas de importância *Birnbaum*, *Criticality* e *Fussell-Vesely*.

Neste capítulo apresenta-se uma metodologia para análise de barreiras de segurança, até ao momento não existente na bibliografia consultada, criando desta forma uma nova abordagem ao problema. Um melhor conhecimento do comportamento deste tipo de bens revela-se de extrema importância, proporcionando aos responsáveis pela sua manutenção e exploração a melhor escolha na tomada de decisões.

Desta forma, o exposto no presente capítulo surge como a base teórica ou de partida para o próximo capítulo, que pretende ser um complemento do actual, e onde se inclui uma aplicação prática da Metodologia RODS a uma barreira de segurança específica, enquadrada na temática da segurança contra incêndios.

CAPÍTULO VI

APLICAÇÃO DA METODOLOGIA

6.1 – Introdução

De forma a verificar a primeira fase da metodologia proposta no Capítulo V (Metodologia RODS), foi seleccionado para o presente estudo um equipamento que assume um papel fundamental na diminuição do risco de incêndio, sendo responsável por colocar nos meios de combate de primeira intervenção (bocas de incêndio tipo carretel ou bocas de incêndio angulares de escada) ou nos sistemas automáticos (*sprinklers*) aquele que é considerado o mais frequente e melhor agente extintor, devido à sua abundância, custo e características físicas para o combate ao fogo: a **Água**.

Na maioria dos casos o efeito pretendido é o de arrefecimento, que se torna mais importante quanto maior for a superfície exposta da água, ou seja, quanto mais pulverizada estiver, melhor será o arrefecimento alcançado. Quando se pretender maiores alcances no combate ao incêndio, a água deverá ser aplicada sob a forma de jacto. Para se poder alcançar qualquer um dos efeitos anteriormente referidos é necessário que o fluído possua uma determinada pressão.

O equipamento escolhido encontra-se instalado na maior parte das instalações industriais, hospitais, edifícios escolares, desportivos e administrativos, assim como em alguns edifícios de habitação. Trata-se de Sistemas de Bombagem de Água Contra Incêndios, mais vulgarmente conhecidos como Centrais de Bombagem, cuja finalidade é precisamente colocar um determinado caudal à pressão desejada nos dispositivos de combate ao incêndio.

Os próximos parágrafos são dedicados à apresentação detalhada deste tipo de sistema, cujo conteúdo é considerado fundamental para a completa compreensão da aplicação prática subsequente.

6.2 – Sistemas de Bombagem

À primeira vista, quando falamos de sistemas de bombagem, somos logo levados a pensar em processos industriais (produção). No entanto, nem todas as bombas se referem a esta finalidade. O presente trabalho refere-se a um tipo de sistema de bombagem específico, pouco referenciado em estudos de fiabilidade, mas de vital importância em qualquer instalação industrial em matéria de gestão do risco. Tal como referido anteriormente, trata-se de sistemas de bombagem de água contra incêndios, inseridos nos sistemas de protecção.

Os sistemas de bombagem de água contra incêndios são sistemas fulcrais nos mais modernos meios de protecção existentes em qualquer instalação industrial, nomeadamente nas redes de extinção automáticas (normalmente designadas por redes de *sprinklers*), nas redes de incêndio armadas (também designadas por redes de carretéis) ou qualquer outro tipo de meio de extinção que utilize a água sob pressão como agente extintor.

6.2.1 – Perspectiva histórica

Para melhor enquadrar o assunto e facilitar a compreensão a quem possa estar de alguma forma afastado da temática e da sua importância, apresentam-se nos próximos parágrafos algumas considerações sobre o tema e sobre o tipo de equipamento em estudo.

Comecemos pelo princípio! De facto, o fogo sempre desempenhou um papel importante para a Humanidade com o seu poder criador, transformador e destruidor, servindo para cozinhar os alimentos, aquecer os habitats, afugentar os animais ou servir para transformar os materiais, tornando-se um elemento comum da vida familiar e económica nas mais diversas actividades comerciais e industriais. Foi porventura uma das maiores descobertas da Humanidade! No entanto, devido a várias razões, o fogo pode tornar-se incontrolável para o homem, passando a designar-se como um incêndio.

Tal como referido anteriormente, no combate a incêndios o agente extintor mais utilizado universalmente é a água, devido não só aos seus efeitos de arrefecimento e inibição da reacção de combustão, como também devido ao seu baixo custo e fácil acessibilidade. Teoricamente para extinguir um incêndio num quilo de madeira (libertação de cerca de 20 kJ) são necessários aproximadamente 80 gramas de água, o que significa que a massa de água para extinguir um incêndio é consideravelmente inferior à massa do combustível, isto não contabilizando a água desperdiçada. Mesmo assim, quando se trata de um incêndio importante, a quantidade de água necessária para o controlar ou extinguir atinge valores elevados, sendo necessário um grande caudal num curto espaço de tempo, dependendo do poder calorífico dos combustíveis.

A história revela factos relacionados com os efeitos destruidores de alguns incêndios importantes (Viegas, 2006), tais como:

- O grande incêndio de Roma (64 AC), onde foram perdidas milhares de vidas e destruídos vários distritos da cidade;
- O grande incêndio de Londres (2 de Setembro de 1666), onde milhares de casas e outros edifícios patrimoniais foram destruídos, deixando mais de 200.000 pessoas sem abrigo;
- O terramoto de Lisboa (1 de Novembro de 1755), onde após o sismo e tsunami registados se seguiu um enorme incêndio que durou cerca de 5 dias, sendo apontados cerca de 30.000 mortos como resultado global da catástrofe;
- O grande incêndio de Chicago (8 de Outubro de 1871), onde um conjunto de erros associados à deficiente avaliação inicial do incêndio resultaram na demora inicial do combate, levando à devastação de uma área de cerca de 860 hectares e ao registo de cerca de 300 vitimas. Todo o centro de Chicago foi destruído com todas as suas actividades culturais, cívicas, comerciais e industriais. A inexistência de água a partir de uma certa altura foi o golpe fatal para o aumento da destruição, mas uma forte chuvada na tarde do segundo dia de catástrofe conseguiu extinguir finalmente o incêndio;
- O incêndio do Chiado em Lisboa (25 de Agosto de 1988), embora de menor dimensão que os relatos anteriores, teve também grande impacto na opinião pública devido à vulnerabilidade desta zona histórica. A estrutura dos edifícios (madeira) e a propagação facilitada entre edifícios fez com que a situação se complicasse. Mais uma vez a água foi o agente extintor por excelência e os sistemas de bombagem o instrumento utilizado para o transporte da mesma até ao incêndio.

Muitos outros incêndios ocorreram e ocorrem diariamente, com repercussões ao nível da continuidade das actividades ou destruição de edifícios e equipamentos, assim como a ocorrência de mortes e feridos ou danos ambientais. De todos eles se retiram lições que promovem a melhoria das acções de combate, quer a nível dos equipamentos, quer dos métodos utilizados.

Embora o termo Bombeiro possa hoje em dia ser conotado com um conjunto de acções e bravura, a sua origem etimológica refere o Bombeiro como "*o homem da bomba*". Também em Portugal a designação de Bombeiro começou a utilizar-se em 1738 para o homem encarregue da bomba (Viegas, 2006). Presume-se que as primeiras bombas tenham sido utilizadas pelos Egípcios cerca de 2000 anos AC, com a finalidade de irrigar os campos. Mais tarde, na Alexandria, foi inventada a primeira bomba para extinção de fogo. Antes do surgimento das bombas centrífugas (inventadas durante a revolução industrial) usavam-se bombas de água recíprocas ou rotativas, operadas manualmente, através do vento ou a vapor.

Hoje em dia é comum projectar e instalar (por imperativo legislativo ou iniciativa própria) sistemas de bombagem de água contra incêndio em determinados edifícios e instalações fabris com vista à sua protecção contra eventos desta natureza. De facto, os sistemas de bombagem são sistemas fulcrais na maior parte dos sistemas de protecção existentes, contribuindo para um combate mais rápido e eficaz.

As bombas de incêndio são utilizadas para elevar, transferir ou aumentar a pressão ou o caudal de água aplicada no combate ao incêndio. Por este motivo, as instalações industriais utilizam com muita frequência sistemas de bombagem. As bombas utilizadas são normalmente do tipo centrífugo, podendo individualmente debitar caudais até cerca de 30.000 l/min.

De acordo com o tipo de instalação a proteger, poderão ser utilizadas bombas normalizadas ou bombas projectadas e fabricadas com características específicas para o fim a que se destinam. De referir que o estudo de fluidos em movimento (*fluid dynamics*) encontra-se associado a esta temática mas, como se afasta dos objectivos traçados, não será alvo de estudo no presente trabalho. Sobre esta matéria poderão ser encontrados inúmeros estudos e obras de referência.

As primeiras referências a nível mundial, sob a forma de códigos ou recomendações sobre sistemas de bombagem de água contra incêndios, aparecem na NFPA (*National Fire Protection Association*), e reportam a 1896. Relativamente às bombas, nem todos os modelos comerciais existentes no mercado são indicados ou permitidos para ser usados nos sistemas de protecção contra incêndios devido aos requisitos necessários, havendo entidades como a UL (*Underwriters Laboratories*), a FM (*Factory Mutual*) ou a NFPA, entre outras, que aprovam e listam determinados modelos específicos para esse fim.

Hoje em dia, aquando de qualquer investigação sobre incidentes relacionados com incêndio, o desempenho do sistema de bombagem de água contra incêndios é normalmente um dos primeiros assuntos a ser analisado.

Nolan (1998) afirma que em 12 dos 100 maiores acidentes industriais relacionados com incêndio, o principal factor que contribuiu para dano em larga escala está relacionado com a falha do sistema de combate a incêndio. Torna-se pois imperativo que estes sistemas sejam projectados, instalados e mantidos de forma a ter uma elevada fiabilidade.

A instalação de sistemas de bombagem contra incêndios pode parecer uma tarefa simples. No entanto, erros básicos ou pressões económicas podem levar a um grande impacto (negativo) durante um incidente dessa natureza. Relativamente às causas de falha de sistemas de bombagem de água contra incêndios, o estudo de Nolan (1998) refere os seguintes dados:

Tabela 6.1 – *Causas de falha em sistemas de bombagem*

Causas de Falha	**Percentagem**
Especificação	44,1%
Alterações após comissionamento	20,6%
Operação e manutenção	14,7%
Projecto e implementação	14,7%
Instalação e comissionamento	5,9%

6.2.2 – A necessidade de sistemas de bombagem

Existem algumas situações que determinam a utilização cada vez maior de sistemas de bombagem de água contra incêndios a nível mundial, nomeadamente (Valentine & Isman, 2006):

- Aumento do número de sistemas de extinção de incêndio automáticos;
- Exigências recentes ao nível das características de caudal e pressão das instalações de extinção de incêndio à base de água;
- Requisitos dos edifícios em altura.

É necessário referir que o sistema de bombagem para cumprir a sua função precisa que a montante exista uma reserva de água com um determinado volume mínimo face às exigências da instalação.

6.2.3 – Características das bombas usadas em sistemas de bombagem de água contra incêndios

As bombas usadas nos sistemas de protecção contra incêndios são projectadas, construídas e instaladas de acordo com determinadas características. Em termos de pressão, convém distinguir três tipos, nomeadamente:

- Pressão de aspiração;
- Pressão de descarga;
- Pressão nominal.

A pressão de aspiração refere-se à pressão manométrica medida imediatamente antes da água entrar na flange de aspiração da bomba. Este valor depende do abastecimento e da sua capacidade para levar a água até ao ponto indicado anteriormente, supostamente com valor positivo, caso contrário, a tubagem de aspiração pode colapsar ou a bomba sofrer danos. Caso este requisito não seja alcançado, deverão ser introduzidas alterações na instalação, como por exemplo, baixar a bomba relativamente ao reservatório de água ou aumentar o diâmetro da tubagem, diminuindo assim a perda de carga.

A pressão de descarga, tal como a de aspiração, também é manométrica e mede o valor da pressão quando a água sai da bomba, através de um manómetro colocado na flange de descarga. A pressão de descarga é função da pressão de aspiração mais a energia adicionada à água pela bomba. Terá que haver uma preocupação para que a tubagem e acessórios a jusante da bomba estejam dimensionados para trabalhar com a pressão produzida. O valor da pressão de descarga varia de acordo com o caudal debitado pela bomba, sendo máximo a caudal zero e mínimo quando a bomba operar ao caudal máximo.

Por fim, a pressão nominal diz respeito à energia que é realmente fornecida pela bomba à água, sendo independente da pressão de aspiração. A única forma de saber a pressão nominal é efectuar a diferença entre a pressão de descarga e a pressão de aspiração.

Outra característica importante é a velocidade de rotação da bomba que influência os valores de pressão e de caudal. Qualquer bomba é fabricada para uma dada pressão nominal e um caudal nominal (à velocidade nominal), o que permite discutir e comparar bombas diferentes e ver qual a que mais se ajusta às necessidades específicas de determinada instalação. Algumas considerações relacionadas com estes parâmetros poderão ser encontradas em documentos de referência nesta matéria, tais como a NFPA 20 (2003) ou a Cepreven (2006). A primeira trata-se de uma Norma para a instalação de bombas estacionárias contra incêndios, tendo sido esta versão tornada Norma Nacional Americana em Julho de 2003. Desde a formação do Comité Técnico em Bombas Contra Incêndio da NFPA em 1899 que esta norma tem sofrido actualizações no sentido de se adequar e abranger novos desenvolvimentos nesta área.

A Cepreven, apesar de ser de origem espanhola tem grande procura e aceitação no nosso país, talvez motivado pelo custo excessivo pago por uma certificação passada por um reconhecido organismo norte-americano para atestar a conformidade com a NFPA 20. Hoje em dia estas barreiras de segurança podem ainda ser construídas tendo em conta outras especificações, como a CEA 4001[20] (2009) ou a EN12845[21] (2009). Não contabilizando as centrais de bombagem não normalizadas instaladas actualmente em Portugal (a maioria, com cerca de 67%), a maior parte dos restantes sistemas de bombagem de água contra incêndios (aproximadamente 95%) segue a referência (Cepreven). Neste documento (Cepreven, 2006) são descritas recomendações para o fabrico e instalação de sistemas de bombagem.

6.2.4 – Tipos de bombas

Tal como referido anteriormente, as primeiras bombas utilizadas no combate a incêndio eram do tipo deslocamento positivo (bombas de pistão ou bombas de carretos rotativos).

[20] Norma Europeia elaborada pelo *Comité Européen des Assurances*, tendo como base a política de prevenção no âmbito segurador e principalmente na área dos *sprinklers*.

[21] Norma Europeia para sistemas fixos de combate a incêndios, sistemas de aspersão automáticos – Projecto, instalação e manutenção.

Actualmente apenas alguns sistemas utilizam este tipo de bombas, tais como sistemas de espuma. A maior parte das bombas de água contra incêndio são do tipo centrífugo, utilizando desta forma a força centrífuga para aumentar a energia da água. Existem também as bombas bipartidas (Figura 6.1), onde a voluta que rodeia o impulsor se encontra dividida em duas partes

Figura 6.1 – Bomba bipartida

Pode-se também referir as bombas *in-line* e as bombas de eixo vertical. Estas últimas podem aspirar a água que se encontra num nível inferior ao da bomba. Normalmente, as bombas auxiliares (também designadas por bombas *jockey*), destinadas a manter a pressão na rede, não necessitam de homologação e poderão ser do tipo multicelular, correspondendo esta designação a bombas com mais do que um impulsor dentro da voluta.

6.2.4.1 – Bombas centrífugas

A classificação mais comum de bombas centrífugas usadas em sistemas de protecção contra incêndios, diz respeito à forma como o veio está orientado. Assim, teremos:

- Bombas centrífugas horizontais;
- Bombas centrífugas verticais.

A Figura 6.2 mostra um dos tipos mais comuns em sistemas de bombagem de água contra incêndios no nosso país (bombas centrífugas horizontais). Em futuros parágrafos será feita também referência aos meios de accionamento das bombas usadas no combate a incêndio.

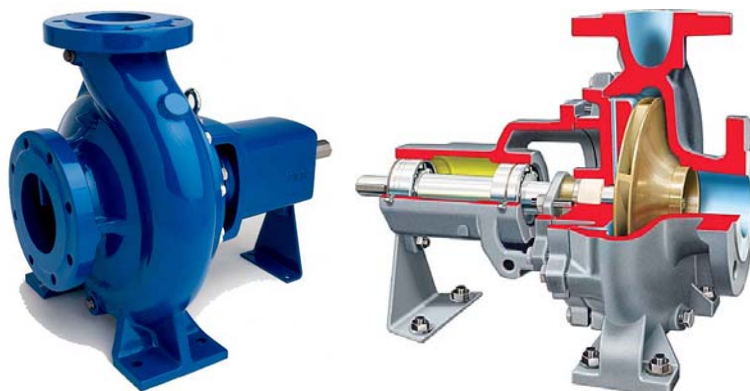



Figura 6.2 – Bomba centrífuga horizontal

6.2.4.2 – Ensaios

A fim de verificar o bom funcionamento dos sistemas de bombagem é necessário efectuar ensaios periodicamente. As referências normativas anteriormente enunciadas prevêem algumas alternativas para realizar fisicamente esses testes, tais como utilizar:

- Um colector de ensaio para várias mangueiras. A água gasta durante o ensaio será desperdiçada, indo para o sistema de drenagem pluvial;
- Colector com dispositivo de medição (caudalímetro), retornando a água ao reservatório de origem;
- Medição em circuito fechado, onde a água passa por um caudalímetro e regressa directamente à aspiração da bomba. É um método pouco desejável, uma vez que não introduz um método de teste ao sistema de abastecimento.

A Norma NFPA 25 (2002) preconiza recomendações para inspecção, ensaio e manutenção. Nestes testes, as bombas são ensaiadas a diversos caudais (lidos no caudalímetro), desde o caudal zero até ao caudal máximo (140% ou 150% do caudal nominal, conforme se refira à Cepreven ou à NFPA, respectivamente).

Em simultâneo com cada valor de cada caudal debitado dever-se-á efectuar a leitura do manómetro a fim de registar a pressão de descarga nesse ponto. As várias leituras dos pares caudal/pressão efectuadas permitem traçar a curva da bomba ou mesmo aferir se a curva fornecida com cada bomba está a ser cumprida. A Figura 6.3 apresenta as curvas características das bombas de acordo com a NFPA 20 e Cepreven, respectivamente.

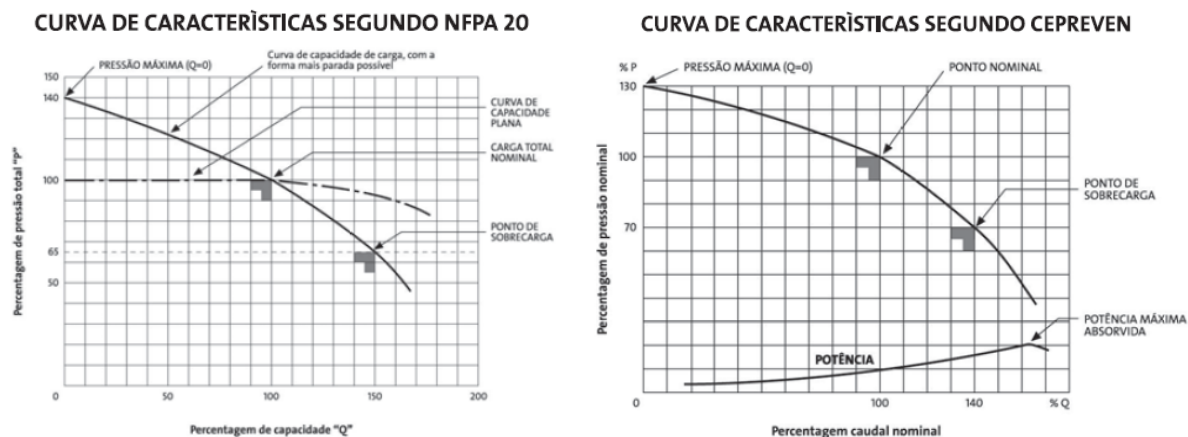



Figura 6.3 – Curvas características segundo NFPA 20 e Cepreven

Como estes sistemas de protecção contra incêndios não são usados com frequência, a única forma de verificar potenciais problemas é através de testes de rotina e de inspecções. Um exemplo referente aos problemas que poderão ocorrer numa central de bombagem é a perda de uma das fases na alimentação do motor devido por exemplo à queda de um raio, pico de tensão ou algo semelhante que danifique um dos condutores. Nesta circunstância a bomba rodava muito lentamente, até à avaria do motor ou do controlador. Os equipamentos mais modernos já informam desta situação ou da inversão de fase, mas muitos equipamentos que se encontram instalados não possuem monitores de fase, podendo ser danificados por um qualquer pico de tensão.

A NFPA 25 – *Inspecção, Testes e Manutenção de Sistemas Hidráulicos de Protecção Contra Incêndio* (2002), embora sem provar cientificamente como se determinam os valores apresentados, especifica:

- A frequência dos testes;
- Como devem ser feitos os testes;
- O que deve ser registado;
- Que formulários devem ser usados para registar os resultados.

Por exemplo, as bombas de incêndio devem ser testadas semanalmente, cerca de 10 ou 30 minutos conforme sejam respectivamente accionadas por motores eléctricos ou motores diesel. Nestes testes também se avalia a perda de fase ou inversão da mesma. Anualmente cada bomba deve ser testada nas condições de caudal mínimo, caudal nominal e caudal máximo. Todas as situações consideradas anormais devem ser anotadas e corrigidas.

6.2.4.3 – Meios de accionamento

As bombas usadas no combate a incêndio podem ter basicamente três meios de accionamento (Valentine & Isman, 2006), nomeadamente:

- Motores eléctricos;
- Motores diesel;
- Turbinas a vapor.

Embora aqui referenciadas, as turbinas a vapor não são actualmente usadas para o accionamento das bombas de incêndio. Assim, apenas os dois primeiros tipos de motor são normalmente utilizados. De referir que até 1974 também estavam disponíveis motores a gasolina, mas, devido à alta volatilidade deste combustível, deixaram de ser aplicados.

Os motores eléctricos apresentam algumas vantagens, tais como a limpeza, a isenção de ruído, o custo, a necessidade de pouca manutenção e a sua dimensão. No entanto, apresentam a desvantagem de necessitarem de energia eléctrica para funcionar. O motor diesel, embora não tenha o condicionalismo apontado para os motores eléctricos, requer ensaios mais frequentes e maiores cuidados de manutenção. De acordo com Valentine e Isman (2006) "… *se o proprietário do edifício decidir ter um motor a diesel, também terá que se comprometer em mantê-lo. Um motor que não tenha manutenção não operará, o que faz dele um motor não fiável.*"

Uma grande parte das centrais de bombagem de água contra incêndios instalada em Portugal possui, para além da electrobomba auxiliar (*jockey*), duas bombas principais, sendo ambas accionadas por motor eléctrico. Segundo informação recolhida através de um dos maiores fabricantes mundiais deste tipo de equipamento, entre 2005 e 2007 (inclusive), este tipo de arquitectura em Portugal representou cerca de 73,1%, sendo seguido com 15,4% por um modelo de centrais de bombagem com duas bombas principais, sendo uma accionada por motor eléctrico e outra por um gerador diesel. As próximas figuras mostram esquemas referentes a centrais de bombagem de água contra incêndios constituídas por duas bombas principais, sendo no primeiro caso (versão A - Figura 6.4) composto por uma electrobomba e uma motobomba diesel e o segundo (versão B - Figura 6.5) por duas electrobombas.

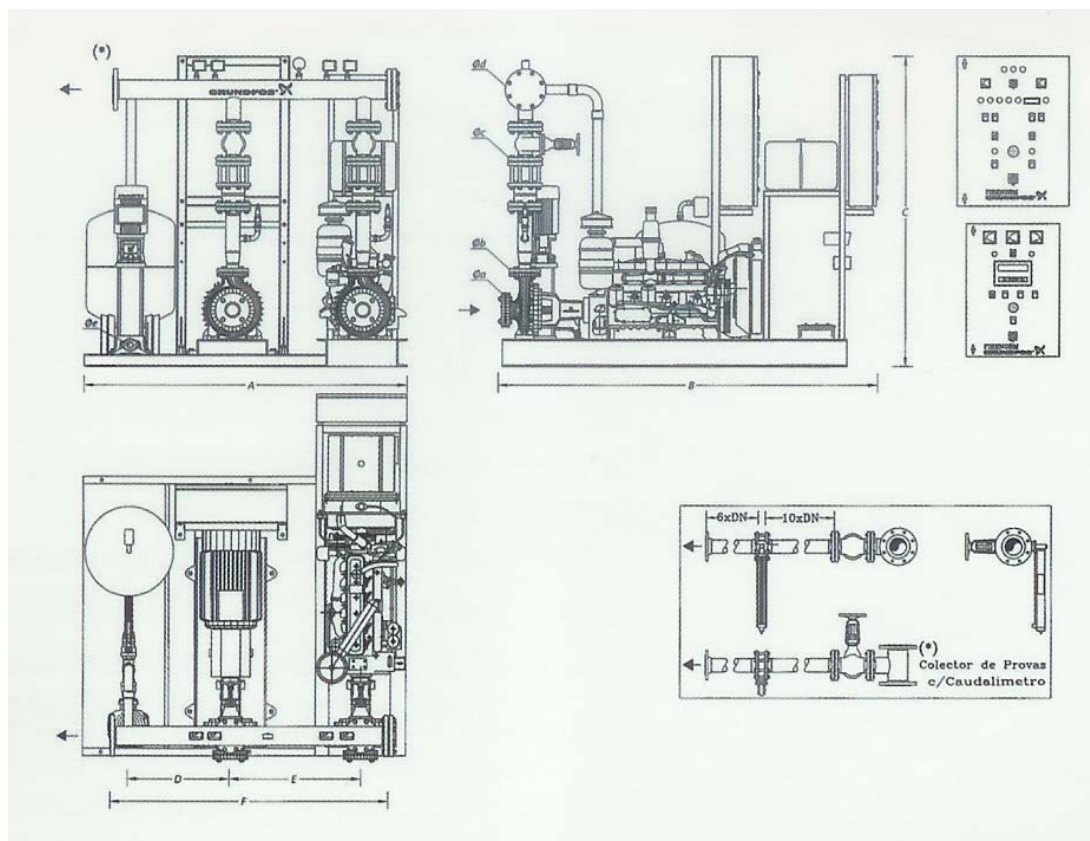



Figura 6.4 – Central de Bombagem Contra Incêndios (versão A)

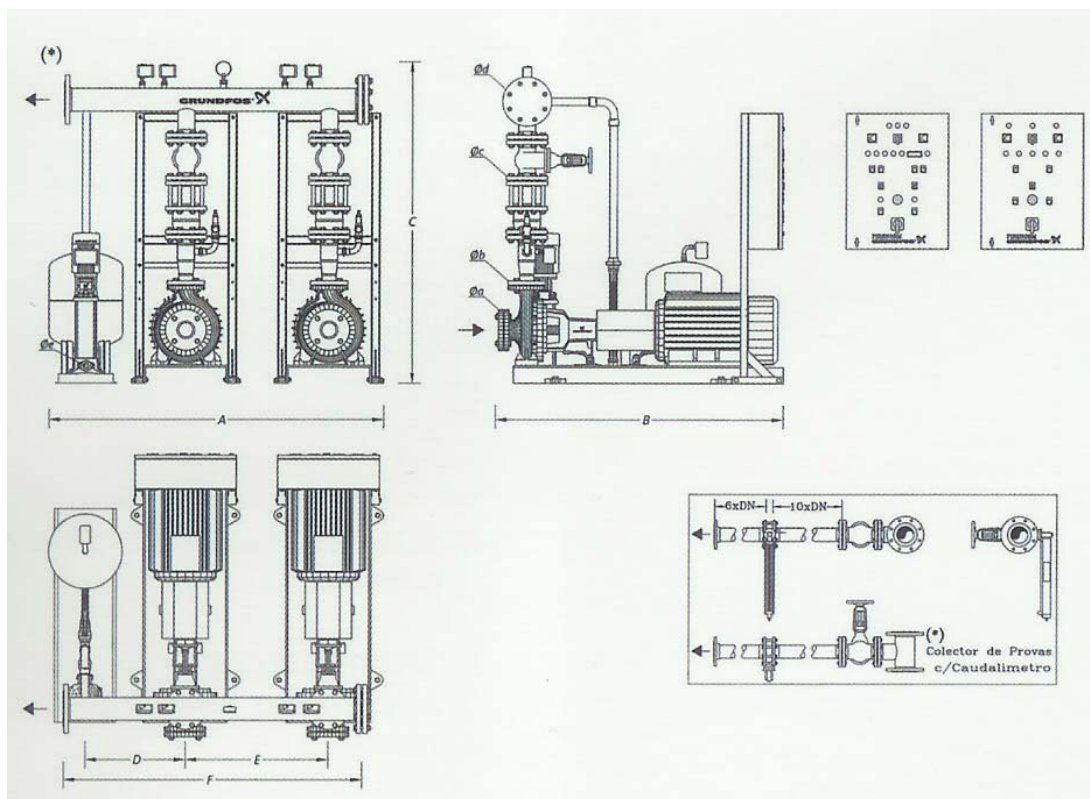



Figura 6.5 – Central de Bombagem Contra Incêndios (versão B)

Relativamente aos controladores e equipamentos das bombas accionadas por motor eléctrico ou motor diesel, a bibliografia anteriormente referenciada (NFPA 20, 2003) (NFPA 25, 2002) apresenta diversa informação relacionada com os requisitos para instalação, inspecção, teste e manutenção das bombas e respectivos accionamentos.

6.2.4.4 – Funcionamento das bombas

A instalação de uma bomba de incêndio começa na fase inicial do projecto, fazendo-se uma avaliação hidráulica do sistema de abastecimento de água proposto e então considerando factores como o caudal, duração e pressão exigidas pelo sistema de protecção contra incêndio, determina-se a necessidade da instalação de uma bomba.

Como referido em parágrafos anteriores, utilizam-se com maior frequência bombas accionadas por motores eléctricos, embora as motobombas diesel confiram uma fonte completamente independente de alimentação, operando com velocidades nominais entre as 1460 e as 3300 rpm. De acordo com a NFPA 20 (2003) só existem dois tipos de abastecimento de energia que podem ser considerados fiáveis, desde que utilizados individualmente, nomeadamente aquele que resulta do fornecimento de uma concessionária pública ou o resultante de um gerador. Ainda de acordo com este documento, os geradores de reserva ou de emergência não podem ser usados como a única fonte de energia eléctrica para bombas de incêndio, mas podem ser usados em combinação com outras formas de fornecimento.

De qualquer uma das formas, a fonte de energia e os cabos condutores eléctricos devem estar protegidos contra fogo ou danos mecânicos. A fonte de alimentação e a bomba devem ser ligados directamente para assegurar que o fornecimento de energia não será interrompido, mesmo no caso de corte geral da instalação.

Para se falar sobre o funcionamento das bombas deve-se referir não só estes equipamentos, mas sim todo o sistema, uma vez que todos os subsistemas se encontram interligados. Quando a central de bombagem se encontra estabilizada, nomeadamente quando se encontra num estado adormecido (*dormant*), com a pressão constante a jusante do sistema, num valor pré-estabelecido e com todos os seus componentes aptos a cumprir as funções para os quais foram projectados, fabricados e instalados, estamos perante uma situação de partida para explicar como é expectável o seu funcionamento.

Nesta situação, quando por qualquer razão a pressão a jusante da central de bombagem baixa até um valor pré-regulado, o pressostato de arranque da electrobomba auxiliar (*jockey*) transmite essa informação a um quadro eléctrico onde, através de encravamentos eléctricos se dá ordem de arranque à electrobomba auxiliar.

Se o caudal fornecido por esta bomba não for o suficiente para contrariar o caudal que está a ser consumido, a pressão continuará a baixar e, chegando a outro patamar de pressão, um outro pressostato de arranque (electrobomba principal) dará essa informação, procedendo-se de forma análoga ao arranque da electrobomba principal.

Caso o pressostato de arranque falhe, existe em redundância um outro pressostato de segurança que cumprirá as funções antes referidas. Quando a pressão continua a baixar (por exemplo por avaria da electrobomba principal), ao se atingir um outro patamar de pressão (inferior), a descrição anterior referente à electrobomba principal repete-se, fazendo então accionar uma segunda electrobomba de reserva ou uma motobomba diesel. A Figura 6.6 mostra uma central de bombagem de água contra incêndio, compacta, com todos os seus componentes.

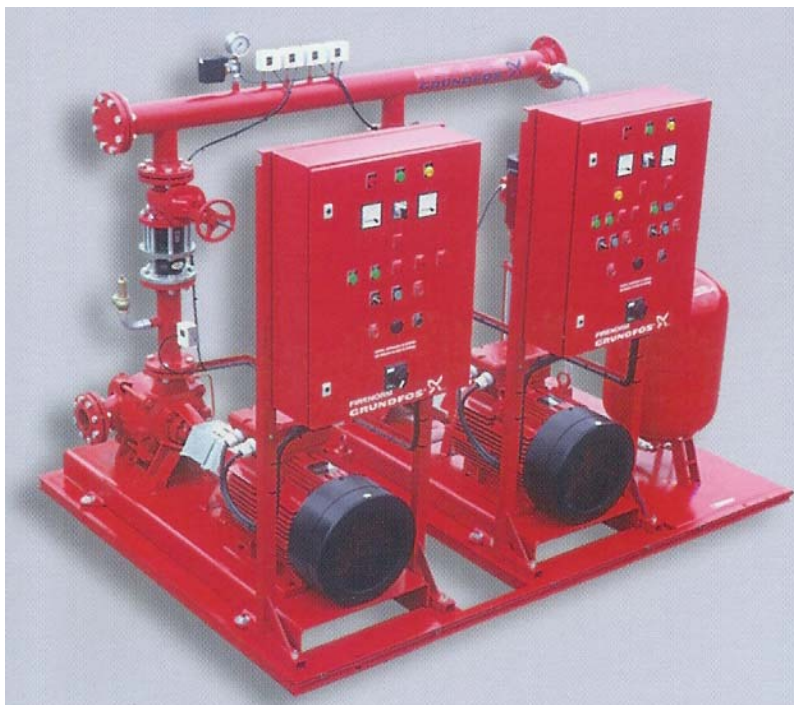



Figura 6.6 – Central de Bombagem de Água Contra Incêndios

Nos sistemas de bombagem de água contra incêndio, se as bombas não funcionam quando é necessário, isso pode representar uma avaria catastrófica da barreira de segurança, ou de várias barreiras de segurança.

Em resultado deste tipo de evento, a legislação (NFPA 20 – *Instalação de Bombas Estacionárias para Protecção contra Incêndio* – Capítulo 10 e 12) (2003) preconiza uma monitorização das bombas contra incêndio. Alguns dos sinais devem ser transmitidos para um local distante, permanentemente ocupado (na eventualidade da bomba não estar num local permanentemente vigiado). Além disso, esta mesma norma exige que o painel junto da central possua pontos de contacto para ligar a circuitos de supervisão e monitorização remota. Esta monitorização remota, no caso de bombas eléctricas, deverá ter sinais separados mostrando as seguintes condições:

- Motor em funcionamento;
- Perda de fase;
- Inversão de fase;
- Ligação do motor a uma outra fonte de energia, quando esta exista.

Para as motobombas diesel, os sinais deverão ser:

- Motor em funcionamento;
- Controlador em posição que não em "automático";
- Defeito no motor ou painel (ex. pressão de óleo muito baixa no sistema de lubrificação, alta temperatura da água na camisa do motor, falha no arranque automático, desligar por excesso de velocidade, falha nas baterias ou falta de bateria, baixa pressão de ar ou hidráulica, alta pressão, problemas de injecção de combustível, baixo nível de combustível e perda de saída no carregador das baterias).

O uso do sistema de alarme para monitorizar todas estas condições pode tornar-se uma opção segura, cruzando as informações recebidas e verificando a integridade do sinal. Assim, de uma forma clara e rápida, pode-se dar algumas garantias que a bomba funcionará quando necessário, ou que se possa responder mais rapidamente a uma avaria, que poderia ser catastrófica. No entanto, será necessário que este sistema de alarme, quando exista, também tenha uma fiabilidade alta. Além disso, haverá a necessidade da existência de meios humanos para supervisão dos sinais, tomada de decisões e execução de testes periódicos ao sistema.

Muitos edifícios de escritórios, escolas, fábricas, lares ou reservatórios de combustível são protegidos por sistemas automáticos ou manuais de extinção de incêndio, ligados a bombas, que podem ficar inactivos durante vários anos até entrarem em operação.

A questão que se normalmente se coloca é: "*Será que estes sistemas funcionarão em caso de incêndio?*". Muitas vezes a resposta obtida é "*não*", pois o sistema de bombagem não chega a funcionar ou pára logo após o arranque, ou por vezes antes do incêndio estar controlado.

Segundo Bill Harvey, da Harvey & Associates (Lewis, 2006), foi o que aconteceu numa fábrica de carpetes, na Geórgia – Carolina do Sul, em 1995. Duas bombas accionadas com motores diesel não funcionaram, tendo o incêndio destruindo toda a fábrica e tendo-se alcançado prejuízos da ordem dos 200 milhões de dólares mas, felizmente, sem vítimas mortais. A investigação realizada *a posteriori* mostrou que as razões para tal falha se deveriam basicamente à falta de procedimentos de manutenção e inspecção adequados para os equipamentos de protecção.

Apesar das normas, códigos e regras para o projecto, instalação, exploração, testes e manutenção de equipamentos de protecção contra incêndios, estes não são normalmente seguidos, dando em muitos casos uma falsa sensação de segurança.

Existem algumas considerações que convêm ser tidas em conta na instalação de uma central de bombagem de águas contra incêndios, nomeadamente:

- Encontrar-se instalada num local de fácil acesso e independente de outras instalações;
- O local da instalação ser ele próprio resistente ao fogo durante um período de tempo não inferior a 60 minutos;
- Possuir sistema de drenagem;
- Terem sido previstos e calculados sistemas de ventilação e renovação de ar, especialmente quando se trata de motores diesel;
- A temperatura ambiente deve situar-se entre o 5ºC e os 40ºC.

Em termos construtivos, dever-se-á ter em consideração que os elementos mecânicos da central de bombagem que se encontram em contacto com a água devam ser de material apropriado, de modo a prevenir a oxidação ou corrosão das partes móveis. O impulsor deve ser construído em bronze ou em aço inoxidável.

6.3 – Caso de estudo prático

Apesar de se tratar de uma barreira de segurança amplamente generalizada e aplicada em todo o mundo, os estudos realizados na óptica da fiabilidade não se encontram efectuados e divulgados nas mesmas proporções. Tal facto deve-se fundamentalmente ao estado específico em que estas barreiras normalmente se encontram ("*dormant*"), não proporcionando dados de vida em quantidade suficiente para o registo e tratamento, e por estas barreiras não se considerarem equipamentos fundamentais para um qualquer processo produtivo.

Na maior parte das instalações industriais de risco elevado estas barreiras são obrigatoriamente vistas com o maior cuidado e atenção pelo Departamento de Segurança ou Departamento de Manutenção. No entanto, esses cuidados apontam fundamentalmente para uma garantia da operacionalidade dos sistemas, recorrendo para tal a uma maior frequência das inspecções, testes e ensaios, mas sem serem efectuados os estudos subsequentes relacionados com a determinação da maior ou menor probabilidade de sucesso, em função dessa frequência.

6.3.1 – Definição da barreira de segurança, função e constituição

De acordo com a Metodologia RODS, e complementando a descrição efectuada nos parágrafos anteriores, considere-se uma central de bombagem de água contra incêndios. Este equipamento será estudado de uma forma generalizada, tendo em vista um equipamento específico, mas sem ser baseado em nenhuma instalação real e concreta.

A barreira de segurança em estudo encontra-se inserida num sistema global de protecção ou combate a incêndios, tendo como função colocar a pressão e caudal necessários em duas redes distintas, nomeadamente numa Rede de Extinção Automática (*sprinklers*) e numa Rede de Incêndio Armada (RIA).

A barreira de segurança em estudo é construída de acordo com a Norma Cepreven (2006), e composta por uma electrobomba auxiliar (*jockey*), uma electrobomba principal e uma motobomba diesel, além de todos os equipamentos e dispositivos inerentes a um equipamento desta natureza.

De acordo com a norma seguida, as duas bombas principais (eléctrica e motor diesel) são de arranque automático, por meio de pressostatos, mas de paragem exclusivamente manual.

A electrobomba auxiliar (*jockey*), de caudal inferior, tem como função principal manter a pressão na instalação devido a possíveis fugas de água no sistema, evitando o arranque da bomba principal devido a pequenas perdas de água não relacionadas com um incêndio. O seu arranque e paragem dão-se de forma automática. Ainda de acordo com a norma de construção da central de bombagem, existem dois quadros eléctricos de comando e controlo, sendo um desses quadros para a bomba principal e para a bomba auxiliar e o outro quadro exclusivamente para a motobomba diesel.

Hidraulicamente, cada bomba principal deve fornecer de forma independente os caudais e pressões exigidos para a instalação. Relativamente às bombas principais, a pressão nominal (altura manométrica total) deverá corresponder ao caudal nominal. A pressão ao caudal zero não deve ser superior a 130% da referida pressão nominal e a bomba deverá ser capaz de debitar um mínimo de 140% do caudal nominal a uma pressão não inferior a 70% da pressão nominal. A Tabela 6.2 apresenta as características nominais dos equipamentos analisados.

Tabela 6.2 – *Características nominais das bombas*

Tipo	Caudal [m^3/h]	Altura manométrica [mca]
Electrobomba Auxiliar	5	90
Electrobomba Principal	120	80
Motobomba Diesel	120	80

Além das bombas e respectivos meios de accionamento, existe um conjunto de equipamentos que se passam a descrever:

- Quadro eléctrico de comando e controlo para a electrobomba principal e electrobomba auxiliar construído de acordo com a EN IEC 60439, incluindo sinalização e comando a 24 V e contactos livres de tensão para transmissão à distância, interruptor tetrapolar de corte geral, sinalizadores de fases, seccionadores e corta circuitos fusíveis, arrancadores estrela-triângulo (P>4 kW), contactor e magneto-térmico para a bomba auxiliar, transformador de tensão, sinalização luminosa e acústica, botoneiras de impulso de paragem, possibilidade de teste de lâmpadas e comutadores de funcionamento (automático, manual e desligado). Além destes equipamentos, existem também aparelhos de medição e

controlo como voltímetro (com comutador), amperímetro para a bomba principal, contador de arranques para a bomba auxiliar, carregador de baterias e baterias de apoio destinadas a assegurar a informação na eventual falha de energia;

- Quadro eléctrico de comando e controlo da motobomba diesel, de acordo com as mesmas exigências que o ponto anterior. Neste caso, existe também um autómato destinado ao comando e informação dos diversos estágios de funcionamento da motobomba, carregador automático de baterias e aparelhagem de medida, como voltímetro e amperímetros de carga para cada bateria;
- Instrumentação e controlo, incluindo manómetro em banho de glicerina, dois pressostatos de arranque por bomba principal, um pressostato de informação de pressão na aspiração e um pressostato de arranque e paragem automática para a bomba auxiliar. Também se inclui uma ligação para um boiador de nível mínimo do(s) reservatório(s), uma válvula de segurança para cada bomba principal, um depósito de membrana de ar pré-comprimido e um medidor de caudal com orifício calibrado;
- Conjunto de componentes hidráulicos, tais como tubagem e acessórios e válvulas de retenção e de seccionamento. Estes componentes deverão ter determinadas especificações e cumprir certos requisitos, tendo especialmente em consideração as pressões máximas de serviço;
- Conjunto de componentes eléctricos, incluindo cabos e respectivas ligações.

As Figuras 6.7 e 6.8 mostram esquemas simplificados da central de bombagem, referentes ao subsistema de aspiração e subsistema de compressão, respectivamente. Os esquemas apresentados representam e identificam as fronteiras de análise.

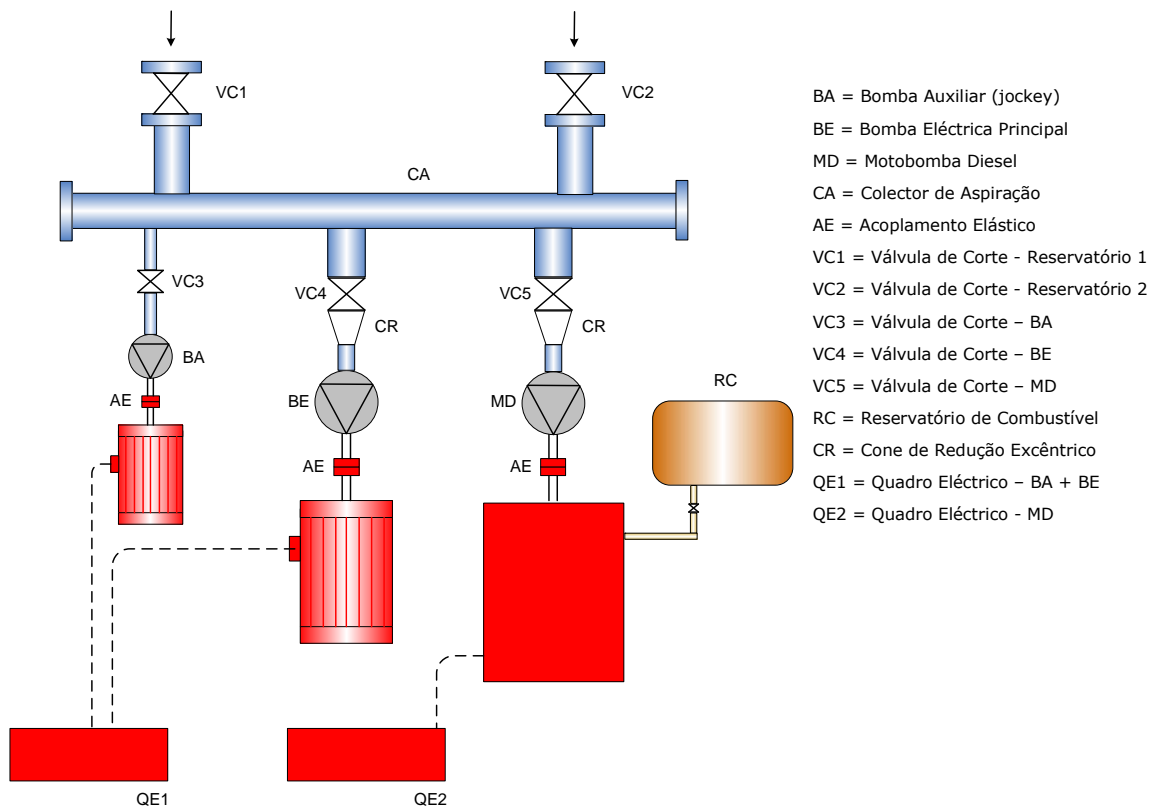



Figura 6.7 – Esquema simplificado do subsistema de aspiração

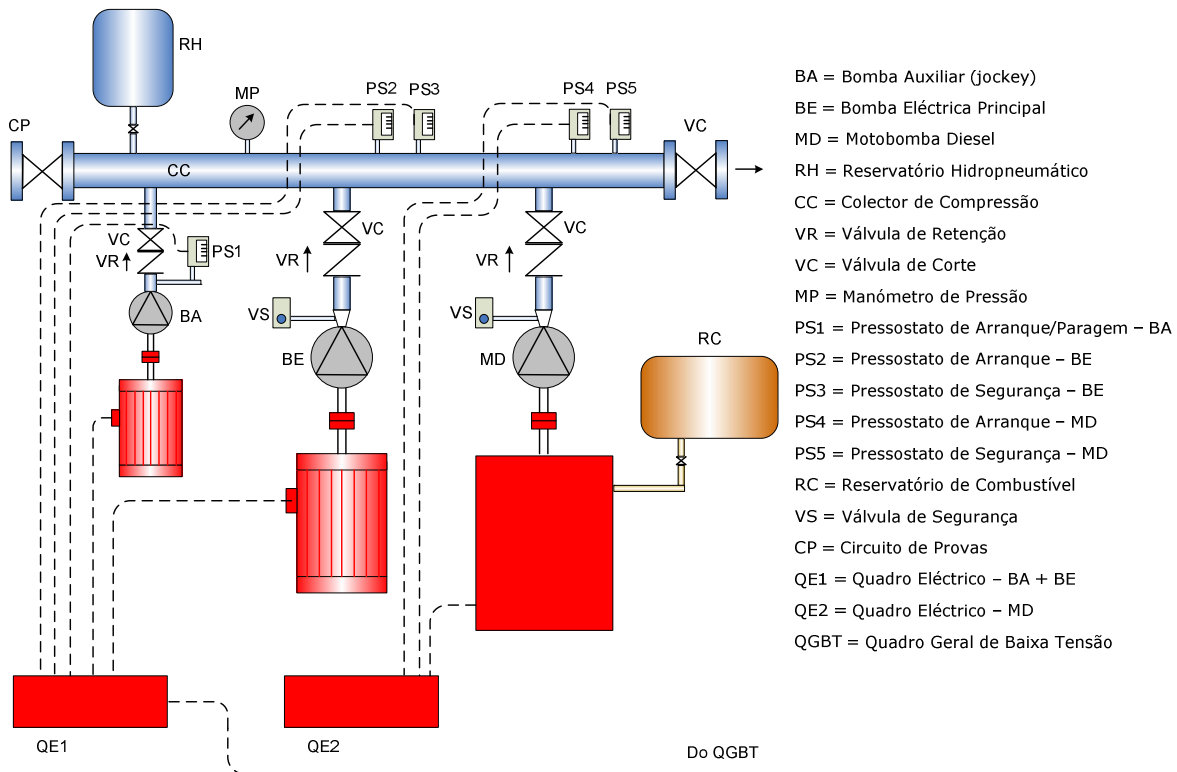



Figura 6.8 – Esquema simplificado do subsistema de compressão

6.3.2 – Identificação dos potenciais acontecimentos de falha dos componentes de suporte

Após a descrição da barreira de segurança e suas características principais há que identificar os componentes que se pretende que se encontrem disponíveis sempre que a barreira de segurança é solicitada, os já designados componentes de suporte (arranque).

Nesta fase é chamada a atenção para uma leitura mais detalhada das normas de construção e das especificações técnicas dos equipamentos, para se obter um conhecimento mais profundo das características e do *modus operandi* deste tipo de sistemas, complementando a informação descrita nos parágrafos anteriores.

Os potenciais modos de falha que se apresentam de seguida referem-se aos componentes de suporte monitorizados, pelo que não serão alvo da análise de fiabilidade, assumindo-se que os mesmos são transmitidos imediatamente após a sua ocorrência, identificados e rapidamente corrigidos.

- Funcionamento deficiente do motor eléctrico devido a perda de fase(s);
- Funcionamento deficiente do motor eléctrico devido a inversão de fases;
- Bomba eléctrica principal em "Não-automático";
- Motobomba diesel em "Não-automático";
- Bomba eléctrica principal desligada;
- Motobomba diesel desligada;
- Falta de água nos reservatórios de abastecimento;
- Baixa pressão do óleo do motor da motobomba diesel.

Considera-se que qualquer um dos modos de falha anteriormente referidos tem um tratamento correctivo imediato, não pondo em causa o arranque da Central de Bombagem de Água Contra Incêndios em situações normais. De igual modo, todas as falhas potenciais referentes à electrobomba auxiliar não são consideradas, uma vez que este equipamento não é destinado ao combate efectivo de um incêndio, tendo outras funções, tal como descrito anteriormente. Desta forma, identificaram-se os Acontecimentos Básicos (AB) referentes aos componentes de suporte não monitorizados, tendo em consideração o princípio de funcionamento da barreira de segurança. Esses Acontecimentos Básicos encontram-se descritos na Tabela 6.3.

Tabela 6.3 – *Identificação dos Acontecimentos Básicos*

AB#	Descrição do Acontecimento Básico
AB1	Falha de Energia da Rede Eléctrica Nacional - 12h/ano
AB2	Falha do Inversor do QGBT
AB3	Falha Interna do Gerador de Emergência
AB4	Falha no Abastecimento de Combustível ao Gerador de Emergência
AB5	Terminais dos Equip. Electromecânicos no Q.E. da Electrobomba Principal Soltos/Partidos
AB6	Falha nos Equip. Electromecânicos do Q.E da Electrobomba Principal
AB7	Cablagem entre o Q.E. da Electrobomba e o Motor Eléctrico interrompida
AB8	Terminais no Motor Eléctrico da Electrobomba Principal Soltos/Partidos
AB9	Falha no Acoplamento entre o Motor Eléctrico e a Bomba da Electrobomba Principal
AB10	Falha no Pressostato de Arranque da Electrobomba Principal
AB11	Falha no Pressostato de Segurança da Electrobomba Principal
AB12	Falha no Estator/Rotor da Electrobomba Principal
AB13	Rolamentos da Electrobomba Principal Gripados/Agarrados
AB14	Válvula de Seccionamento à Saída do Colector de Compressão Fechada - Erro Humano
AB15	Impulsor da Electrobomba Principal Preso
AB16	Terminais dos Equip. Electromecânicos no Q.E. da Motobomba Diesel Soltos/Partidos
AB17	Falha nos Equip. Electromecânicos do Q.E da Motobomba Diesel
AB18	Falha no Acoplamento entre o Motor Diesel e a Bomba da Motobomba Diesel
AB19	Falha no Pressostato de Arranque da Motobomba Diesel
AB20	Falha no Pressostato de Segurança da Motobomba Diesel
AB21	Impulsor da Motobomba Diesel Preso
AB22	Motor Diesel da Motobomba Diesel Gripado/Agarrado
AB23	Falha da Bateria "A" da Motobomba Diesel
AB24	Falha da Bateria "B" da Motobomba Diesel
AB25	Falha das Escovas do Motor de Arranque da Motobomba Diesel
AB26	Falta de Combustível no Depósito da Motobomba Diesel
AB27	Combustível Congelado no Depósito ou nas Tubagens de Ida e Retorno
AB28	Combustível Deteriorado no Depósito da Motobomba Diesel
AB29	Tubagens de Ida/Retorno do Dep. de Combustível Interrompidas ou Desligadas

Relativamente às periodicidades com que os ensaios e testes são efectuados, a prática normal para esta barreira de segurança assenta fundamentalmente em três situações distintas. De acordo com as indicações de fabricantes e alguma experiência na manutenção deste tipo de equipamentos, estipularam-se os seguintes tempos:

- Ensaio ou teste do Gerador de Emergência – Anual
- Ensaio ou teste da Electrobomba Principal - Trimestral
- Ensaio ou teste da Motobomba Diesel – Semestral

Será com base nestas periodicidades que os acontecimentos básicos referentes a cada um dos equipamentos serão alvo de ensaios ou testes de funcionamento e operacionalidade.

6.3.3 – Construção da Árvore de Falhas

Tendo por base os modos de falha básicos identificados no ponto anterior, e dando seguimento à Metodologia RODS, é elaborada uma Árvore de Falhas, onde se estabelece como acontecimento de topo a "***Falha no Arranque da Central de Bombagem de Água Contra Incêndios***". Nesta Árvore de Falhas os acontecimentos básicos são combinados e agrupados de acordo com a sua dependência ou interdependência do ponto de vista funcional, utilizando portas lógicas estáticas ou dinâmicas, assim como a simbologia padronizada relativa aos acontecimentos. Para a realização desta etapa, e a partir deste ponto, recorreu-se à utilização de um software destinado a análises de fiabilidade (Relex 2009®, 2009), seleccionado entre os vários programas informáticos existentes, tendo por base as suas características e capacidades, quer para efectuar a análise qualitativa, quer a análise quantitativa de Árvore de Falhas, e de acordo com as necessidades teóricas enunciadas nos capítulos anteriores.

No momento em que este estudo se encontra a ser realizado, o software utilizado é o único produto comercial para análise de fiabilidade que suporta portas lógicas dinâmicas (*Functional Dependency*, *Sequence-Enforcing e Spare Gate*) no módulo de análise de Árvore de Falhas, possibilitando também o cálculo de indisponibilidade e a análise de medidas de importância. Este software possui a capacidade de transformar as entidades dinâmicas em modelos de Markov equivalentes através de um motor de cálculo interno, produzindo cálculos exactos. De referir que não foi possível utilizar o software Galileo (2004) referido no Capítulo II (gentilmente cedido por investigadores da Universidade da Virginia - USA) por este não permitir o cálculo da indisponibilidade do sistema, nem de outras informações importantes, apesar da ferramenta em causa também contemplar a utilização de portas lógicas dinâmicas. É de salientar que de todos os programas informáticos analisados, só os dois anteriormente referidos possuem esta capacidade.

O resultado final (construção gráfica) relativo à construção da Árvore de Falhas da barreira de segurança em estudo, utilizada para a primeira fase da Metodologia RODS, pode ser analisado com detalhe no **Anexo V**.

Da realização da Árvore de Falhas, e tendo por base os acontecimentos básicos e as portas lógicas usadas na sua construção, resultam diversos Acontecimentos Intermédios (AI), tal como apresentados na Tabela 6.4.

Tabela 6.4 – *Acontecimentos Intermédios da Árvore de Falhas*

AI#	Descrição do Acontecimento Intermédio
AI1	Falha dos Equipamentos de Bombagem
AI2	Falha no Arranque da Electrobomba Principal
AI3	Falha no Arranque da Motobomba Diesel
AI4	Falha de Energia no Quadro Eléctrico da Electrobomba Principal
AI5	Falha na Transmissão de Potência do Quadro Eléctrico para o Motor Eléctrico
AI6	Falha dos Sensores de Pressão da Electrobomba Principal
AI7	Falha no Motor Eléctrico da Electrobomba Principal
AI8	Falha de Energia da Rede de Emergência
AI9	Falha do Gerador de Emergência
AI10	Falha na Transmissão de Potência do Quadro Eléctrico para o Motor Diesel
AI11	Falha dos Sensores de Pressão da Motobomba Diesel
AI12	Falha do Motor Diesel
AI13	Falha do Motor de Arranque da Motobomba Diesel
AI14	Falha das Baterias de Arranque da Motobomba Diesel
AI15	Falha na Alimentação de Combustível à Motobomba Diesel

Na construção da Árvore de Falhas procurou-se encontrar dependências e sequências funcionais entre os seus acontecimentos, o que obrigaria a utilizar portas lógicas dinâmicas. No entanto, por questões de simplificação do modelo, também houve a preocupação de tentar transformar, sempre que possível, essas situações em Árvores estáticas.

De facto, após várias tentativas em estruturar a Árvore de Falhas de forma a que esta traduzisse o mais fielmente possível o modelo real em termos funcionais, havia apenas duas situações em que potencialmente se poderiam utilizar portas lógicas dinâmicas. Estas situações diziam respeito aos sensores de pressão, quer da electrobomba principal, quer da motobomba diesel, uma vez que se poderia considerar o pressostato de segurança como um "*spare*" do pressostato de arranque, com um "*dormancy factor*" igual a 1 (*hot spare*).

Essas situações, correspondentes a sub-Árvores de Falhas dinâmicas, poderiam ser representadas como se indica nas Figuras 6.9 e 6.10.

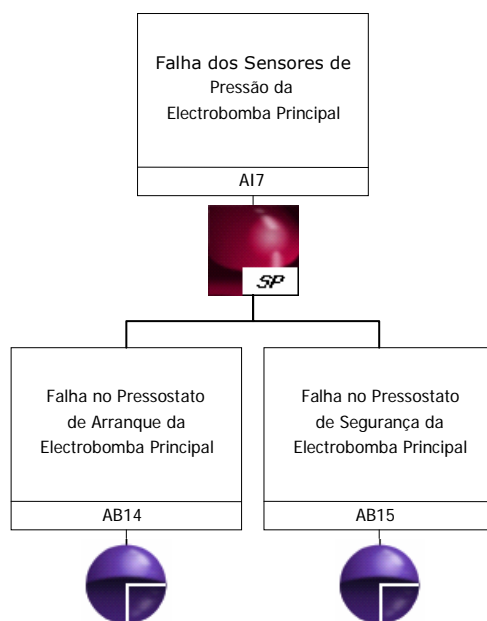



Figura 6.9 – Sub-Árvore de Falhas Dinâmica #1

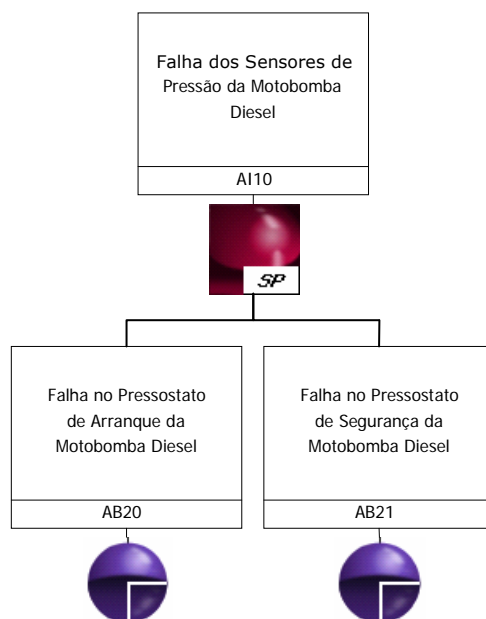



Figura 6.10 – Sub-Árvore de Falhas Dinâmica #2

Embora tal pudesse ser justificado e fundamentado, constatou-se que as situações em causa poderiam ser representadas através de sub-Árvores de Falhas estáticas utilizando a porta lógica "*AND*". No fundo, os pressostatos encontram-se sujeitos a iguais esforços e em cada um dos casos referidos só com a falha dos dois elementos sensores de pressão

ocorrerá a falha do acontecimento intermédio de nível superior, não se registando dependência ou sequência funcional. Considerar o pressostato de segurança um sobressalente do pressostato de arranque não será então o mais correcto, já que ambas as unidades se encontram funcionalmente instaladas em paralelo e muitas vezes não se distingue muito bem qual o pressostato de arranque e qual o de segurança.

Assim, para este equipamento específico não se verificou a necessidade de utilização de portas lógicas dinâmicas, considerando-se todos os acontecimentos como independentes. Depois de estabelecida a estrutura da Árvore de Falhas, poder-se-á então avançar para as análises qualitativa e quantitativa, seguindo a metodologia proposta para este tipo de barreiras de segurança.

6.3.4 – Análise qualitativa da Árvore de Falhas

A análise qualitativa da Árvore de Falhas baseia-se na determinação dos conjuntos de corte mínimos (MCS). Quando esta análise é realizada obtem-se uma listagem com as combinações possíveis de acontecimentos que levam ao acontecimento intermédio ou acontecimento de topo, conforme o nível de análise que se pretenda, tendo em conta as portas lógicas utilizadas na construção da Árvore de Falhas.

Por exemplo, para o Acontecimento Intermédio nº13 (AI13)[22], os conjuntos de corte mínimos são:

- {AB25}
- {AB23, AB24}

O que significa que para este exemplo em particular a falha do motor de arranque da motobomba diesel ocorre quando se verificar falha nas escovas do motor de arranque ou quando falharem as baterias "A" **e** "B".

Relativamente ao acontecimento de topo (AT), cuja determinação dos conjuntos de corte mínimos é o objectivo principal da análise qualitativa, uma vez que reflecte todas as combinações possíveis que levam à falha no arranque da central de bombagem de água contra incêndios, é apresentada uma listagem completa desses conjuntos de corte mínimos no **Anexo VI**.

[22] Ver Anexo V

Da leitura desta listagem podem-se retirar algumas conclusões significativas. De facto, analisando a importância de cada conjunto de corte, relacionada directamente com a ordem do mesmo, verifica-se a existência de apenas 1 (um) conjunto de corte de primeira ordem, 80 (oitenta) conjuntos de segunda ordem, 56 (cinquenta e seis) conjuntos de terceira ordem e apenas 8 (oito) conjuntos de quarta ordem.

Assim, dever-se-á dar fundamental importância ao acontecimento relacionado com o conjunto de corte de primeira ordem, que no presente estudo se refere com uma avaria de causa comum (CCF) relacionada com erro humano, e que corresponde à situação de inadvertidamente se deixar a válvula de seccionamento à saída do colector de compressão fechada.

Deste facto resulta a falha no arranque da central de bombagem de água contra incêndios, uma vez que o abaixamento da pressão na rede de extinção não é detectado pelos pressostatos de arranque e segurança, quer da electrobomba principal, quer da motobomba diesel. Infelizmente esta é uma situação que ocorre com alguma frequência, inviabilizando a primeira fase funcional da barreira de segurança. Normalmente esta situação ocorre após uma intervenção de manutenção, teste ou ensaio, ou por acto deliberado ou intencional.

Numa análise meramente qualitativa, seguem-se em importância outros conjuntos de corte (segunda ordem), ou combinações de acontecimentos, que deverão ser analisados com o objectivo de encontrar soluções para a sua eliminação. Estas soluções passam por incluir redundâncias, dispositivos de alerta ou outras situações que sejam fisica e economicamente viáveis.

Nesta análise qualitativa não são calculadas as probabilidades de ocorrência de cada um desses conjuntos de corte, ignorando qualquer informação numérica relativa aos acontecimentos básicos. O cálculo das probabilidades é realizado aquando da análise quantitativa, que é apresentada nos próximos parágrafos.

6.3.5 – Análise quantitativa da Árvore de Falhas

Por forma a ser efectuada a análise quantitativa da Árvore de Falhas, e dessa forma ser determinada a indisponibilidade associada a cada acontecimento (e fundamentalmente a

que se refere ao acontecimento de topo), é necessário conhecer alguns parâmetros relacionados com cada acontecimento básico identificado aquando a elaboração da Árvore de Falhas, nomeadamente taxas de avarias e intervalos de tempo entre testes ou ensaios.

Assim, todos as falhas mencionadas para os acontecimentos básicos relacionados com a electrobomba principal serão no limite detectadas de três em três meses, as falhas relacionadas com a motobomba diesel de seis em seis meses e as referentes ao gerador de emergência anualmente.

A Figura 6.11 mostra uma imagem do programa informático utilizado (Relex 2009®, 2009), já referido em 6.3.3, com o menu de entrada típico para introdução de dados referentes a cada acontecimento básico.

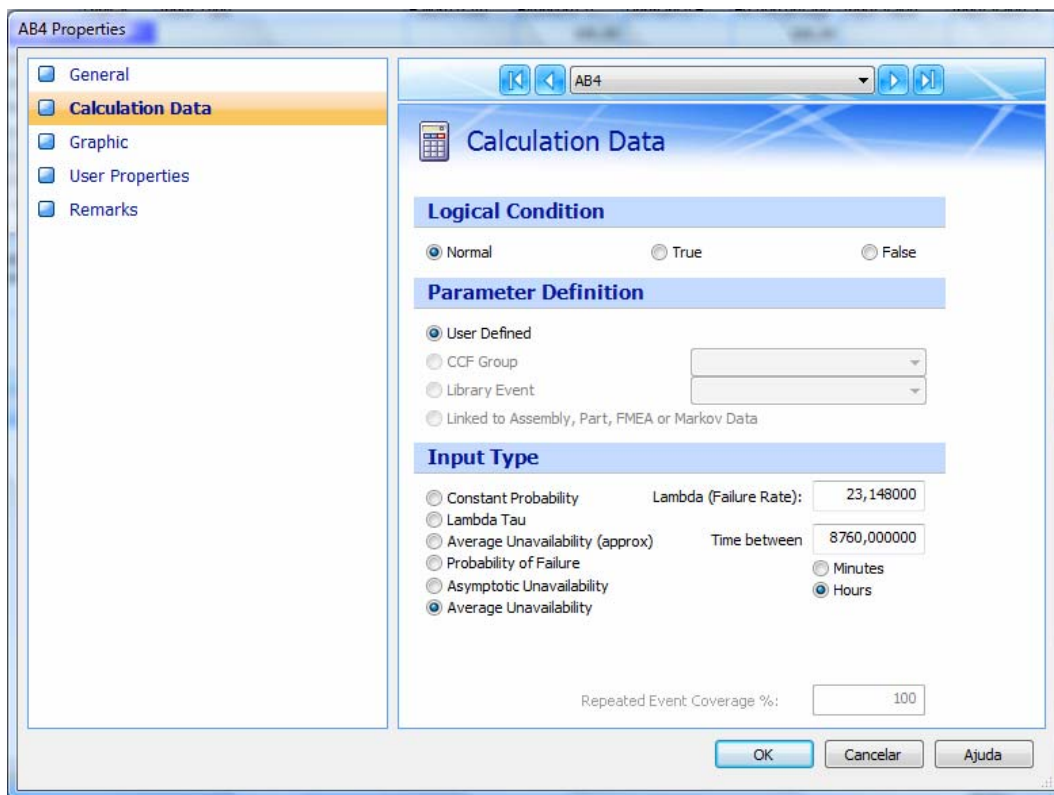



Figura 6.11 – Menu de entrada de dados

De referir que o tipo de entrada (*Input Type*) seleccionado, "*Average Unavailability*" conduz a um cálculo exacto da indisponibilidade. Este modelo é mais indicado quando os equipamentos seguem manutenções preventivas regulares, e particularmente quando se

realizam testes ou ensaios periodicamente, como é o caso prático em estudo. Neste tipo de entrada o tempo relativo à execução das acções (testes ou ensaios) são considerados negligenciáveis, tal como assumido nos pressupostos da Metodologia RODS.

A indisponibilidade associada a cada acontecimento varia entre "0" e "τ", dependendo do tempo a que a avaria ocorre. Neste modelo, os cálculos produzidos reflectem resultados exactos da indisponibilidade média do acontecimento durante o intervalo de teste ou ensaio, utilizando para tal a expressão (4.39). Desta forma o programa informático utilizado possibilita a aplicação da teoria explicitada nos capítulos anteriores, indo ao seu encontro quanto aos fundamentos enunciados.

A Tabela 6.5 indica os valores introduzidos no programa informático para cada um dos acontecimentos básicos identificados aquando da estruturação do modelo referente à barreira de segurança. É importante referir que as taxas de avaria apresentadas resultam da informação prestada por um fabricante de bombas e não de dados fidedignos de campo relativos a alguma situação em particular. Apesar de nesse aspecto não se tratarem de valores bem fundamentados, houve a intenção de colocar dados o mais próximos possível da realidade e dessa forma permitir exemplificar a metodologia proposta.

Tabela 6.5 – *Parâmetros de entrada para o cálculo da indisponibilidade*

AB#	λ [av/10^6 horas]	τ [horas]
AB1	(*)	
AB2	23,148	8760
AB3	16,534	8760
AB4	23,148	8760
AB5	12,860	2160
AB6	28,935	2160
AB7	7,716	2160
AB8	9,645	2160
AB9	19,290	2160
AB10	57,870	2160
AB11	38,580	2160
AB12	7,716	2160
AB13	9,645	2160
AB14	115,741	2160
AB15	12,860	2160

AB#	λ [av/10^6 horas]	τ [horas]
AB16	12,860	4320
AB17	28,935	4320
AB18	23,148	4320
AB19	38,580	4320
AB20	23,148	4320
AB21	12,860	4320
AB22	9,645	4320
AB23	57,870	4320
AB24	57,870	4320
AB25	28,935	4320
AB26	38,580	4320
AB27	2,315	4320
AB28	9,645	4320
AB29	23,148	4320

(*) Considerada uma indisponibilidade média de 12 horas por ano

Após a introdução dos dados anteriores pode agora ser determinada a indisponibilidade média associada aos acontecimentos intermédios e ao acontecimento de topo, alcançando-se assim o objectivo traçado para a primeira fase da Metodologia RODS.

Desta forma, verificou-se uma indisponibilidade média para o acontecimento de topo, ou seja, a indisponibilidade média associada à falha no arranque da central de bombagem de água contra incêndios, de **0,1497**. Este é o valor que traduz a probabilidade de não ocorrer uma transição positiva em termos funcionais da primeira fase para a segunda fase de operação da Central de Bombagem, tal como descrito na Metodologia RODS.

Para uma compreensão mais completa dos factores de influência que levam ao resultado alcançado, analisaram-se também as indisponibilidades médias associadas aos acontecimentos intermédios, tal como apresentado na Tabela 6.6.

Tabela 6.6 – *Indisponibilidade média associada aos acontecimentos intermédios*

AI#	Indisponibilidade média
AI1	0,039007
AI2	0,112867
AI3	0,345602
AI4	0,000325
AI5	0,080959
AI6	0,002431
AI7	0,018546
AI8	0,237304
AI9	0,157364
AI10	0,129842
AI11	0,003816
AI12	0,223909
AI13	0,072450
AI14	0,013272
AI15	0,145737

De igual forma, apresentam-se na Tabela 6.7 as indisponibilidades médias associadas a cada acontecimento básico, que no fundo resultam da aplicação da expressão (4.39), tendo em conta os parâmetros individuais (λ,τ). Os resultados apresentados reflectem a propensão para a ocorrência de avarias ocultas, sendo também influenciados pelo período entre testes ou ensaios, que quanto mais alargado for, maior será o valor da indisponibilidade média.

Tabela 6.7 – *Indisponibilidade média associada aos acontecimentos básicos*

AB#	Indisponibilidade média	AB#	Indisponibilidade média
AB1	0,001370	AB16	0,027270
AB2	0,094869	AB17	0,059975
AB3	0,069046	AB18	0,048374
AB4	0,094869	AB19	0,078890
AB5	0,013761	AB20	0,048374
AB6	0,030609	AB21	0,027270
AB7	0,008287	AB22	0,020547
AB8	0,010345	AB23	0,115202
AB9	0,020547	AB24	0,115202
AB10	0,059975	AB25	0,059975
AB11	0,040533	AB26	0,078890
AB12	0,008287	AB27	0,004984
AB13	0,010345	AB28	0,020547
AB14	0,115203	AB29	0,048374
AB15	0,013761		

Da interpretação dos resultados alcançados ressaltam algumas constatações, nomeadamente o valor da indisponibilidade média referente ao acontecimento de topo (aprox. 15%), as indisponibilidades médias relativas aos acontecimentos intermédios AI3 (Falha no Arranque da Motobomba Diesel), AI8 (Falha de Energia da Rede de Emergência) e AI12 (Falha do Motor Diesel).

Também a informação referente à indisponibilidade média relativa aos acontecimentos básicos tem algumas situações que se destacam pelos valores alcançados, nomeadamente o acontecimento básico AB14 (Válvula de Seccionamento à Saída do Colector de Compressão Fechada - Erro Humano), AB23 (Falha da Bateria "A" da Motobomba Diesel) e AB24 (Falha da Bateria "B" da Motobomba Diesel).

De qualquer forma, não se pode olhar apenas para o valor relativo das indisponibilidades médias, uma vez que esta importância deriva em larga escala da estrutura da Árvore de Falhas e do tipo das portas lógicas utilizadas.

6.3.6 – Outros dados importantes

Tal como referido no capítulo anterior, relativo à descrição da Metodologia RODS, existem outros dados importantes que se podem retirar do estudo efectuado, e que complementam a análise quantitativa. Trata-se de saber as medidas de importância

(*Importance Measures*), ao se proceder a uma análise de sensibilidade. Só desta forma ficaremos a saber, por exemplo, o contributo individual de cada acontecimento básico para o valor da indisponibilidade média alcançada para o acontecimento de topo.

No seguimento da análise efectuada ao caso em estudo, e tendo por base as indicações e aplicabilidades referentes a cada uma das medidas de importância apresentadas no capítulo anterior, pretende-se saber qual a probabilidade com que cada um dos acontecimentos básicos contribuiu para a ocorrência do acontecimento de topo. Assim, analisou-se a medida de importância *Fussell-Vesely*, justificada em virtude dos objectivos pretendidos, conforme descrito no Capítulo V. De acordo com esta medida de importância, a Tabela 6.8 mostra de uma forma hierarquizada o contributo de cada acontecimento básico para a ocorrência do acontecimento de topo.

Tabela 6.8 – *Medida de importância Fussell-Vesely*

AB#	*Fussell-Vesely*	AB#	*Fussell-Vesely*
AB14	0,701295	AB21	0,019709
AB6	0,077009	AB22	0,014850
AB26	0,057017	AB28	0,014850
AB9	0,051694	AB24	0,009592
AB25	0,043346	AB23	0,009592
AB17	0,043346	AB10	0,006116
AB29	0,034962	AB11	0,006116
AB18	0,034962	AB27	0,003602
AB5	0,034622	AB19	0,002758
AB15	0,034622	AB20	0,002758
AB8	0,026026	AB1	0,000892
AB13	0,026026	AB4	0,000327
AB7	0,020850	AB2	0,000327
AB12	0,020850	AB3	0,000238
AB16	0,019709		

Desta forma pode-se concluir que o grande contribuinte para o valor da indisponibilidade associada à falha no arranque da central de bombagem de água contra incêndio é o potencial erro humano referente à situação da válvula de seccionamento à saída do colector de compressão se encontrar fechada (AB14). Embora com uma grande diferença percentual, seguem-se outros acontecimentos básicos, como o AB6 (Falha nos Equipamentos Electromecânicos do Q.E. da electrobomba Principal), AB26 (Falta de Combustível no Depósito da Motobomba Diesel) e AB9 (Falha no Acoplamento entre o Motor Eléctrico e a Bomba da Electrobomba Principal).

Este tipo de análise também confirma algo que foi referido anteriormente, nomeadamente quando se afirma que não se devem olhar para as indisponibilidades individuais quando se pretende saber a influência dos correspondentes acontecimentos básicos no valor determinado para a indisponibilidade média do acontecimento de topo. Os acontecimentos AB6, AB26 e AB9 referidos anteriormente como maiores contribuintes a seguir ao AB14, apresentavam indisponibilidades médias individuais relativamente baixas (3,1%, 7,9% e 2,1%, respectivamente). Da mesma forma, constata-se que alguns acontecimentos básicos que apresentavam indisponibilidades médias mais elevadas não têm de certa forma um papel tão preponderante quando se analisam as medidas de importância.

6.3.7 – Critério de aceitação do risco

Mas será que para a barreira de segurança em causa um valor de indisponibilidade média de 0,1497 é um valor aceitável? De facto, este é um tipo de questão que se coloca e que não é de fácil resposta. Tudo depende do risco que se pretenda assumir, do tipo de actividade industrial em causa e do critério aplicável. Desta forma, justifica-se o enquadramento que se efectuou nos capítulos iniciais deste trabalho, nomeadamente quando se descreveu com detalhe a Metodologia RAMS[23] e quando se referiram critérios de aceitação do risco[24]. Poder-se-á desta forma aplicar um dos critérios de aceitação enunciados, e com base nos valores alcançados decidir quanto à sua aceitação. De referir que o critério ALARP é um dos mais utilizados quando se aborda este tipo de questões.

Como esta é uma matéria que deve ser debatida no seio de cada organização, estipulando-se quais as regiões, limites ou fronteiras de não aceitação do risco, não será desenvolvida no presente estudo qualquer aplicação quantitativa. De facto, a tolerabilidade do risco subjacente à indisponibilidade de uma barreira de segurança é um assunto a ser amplamente discutido e assente em bases sólidas e bem definidas. Mesmo em situações de risco aceitável dever-se-ão estipular as medidas que permitam manter o risco a esse nível, evitando que o mesmo sofra grandes alterações ao longo do tempo. Quando não aceitável, a redução do risco deverá ser equacionada tendo em atenção as análises qualitativas e quantitativas efectuadas. O importante a reter nestes parágrafos é

[23] Ver Capítulo II

[24] Ver Capítulo III – 3.2.1

mostrar a necessidade de se estabelecer um critério de aceitação do risco após a realização de uma análise quantitativa.

6.3.8 – Simulação para cenários alternativos

Seguindo as ideias apontadas nos parágrafos anteriores, e no pressuposto de que o valor encontrado para a indisponibilidade da barreira de segurança conduz a um risco não aceitável, procedeu-se à simulação de alguns cenários alternativos. Tais cenários passam fundamentalmente por se observar dois tipos de alterações face ao cenário inicial (designado por "Cenário 1"), nomeadamente:

- Alteração das periodicidades para a realização dos testes e ensaios a alguns sistemas da barreira de segurança;
- Melhoria de alguns parâmetros individuais.

Desta forma, criaram-se mais cinco cenários, reflexo de algumas alterações, tal como indicado na Tabela 6.9.

Tabela 6.9 – *Cenários alternativos*

Cenário#		Condições
Cenário 2	Manutenção – Ensaios – Gerador de Emergência	Periodicidade – Anual
	Manutenção – Ensaios – Electrobomba Principal	Periodicidade - Mensal
	Manutenção – Ensaios – Motobomba Diesel	Periodicidade - Semestral
Cenário 3	Manutenção – Ensaios – Gerador de Emergência	Periodicidade – Anual
	Manutenção – Ensaios – Electrobomba Principal	Periodicidade - Trimestral
	Manutenção – Ensaios – Motobomba Diesel	Periodicidade - Trimestral
Cenário 4	Manutenção – Ensaios – Gerador de Emergência	Periodicidade – Semestral
	Manutenção – Ensaios – Electrobomba Principal	Periodicidade – Trimestral
	Manutenção – Ensaios – Motobomba Diesel	Periodicidade - Semestral
Cenário 5	Manutenção – Ensaios – Gerador de Emergência	Periodicidade – Anual
	Manutenção – Ensaios – Electrobomba Principal	Periodicidade – Mensal
	Manutenção – Ensaios – Motobomba Diesel	Periodicidade - Trimestral
Cenário 6	Válvula à saída do colector de compressão	Indicação de posição

Assim, para o "Cenário 2", a alteração das condições face ao "Cenário 1" passa por efectuar testes ou ensaios à Electrobomba Principal mensalmente em vez de trimestralmente.

No "Cenário 3", a alteração das condições face ao "Cenário 1" passa por efectuar testes ou ensaios à Motobomba Diesel trimestralmente em vez de semestralmente.

Para o "Cenário 4" apenas se alterou a periodicidade dos testes ou ensaios do Gerador de Emergência para semestral em substituição da periodicidade anual.

Para o "Cenário 5" foram as periodicidades dos testes ou ensaios da Electrobomba Principal e Motobomba Diesel, que passaram a ser efectuados mensalmente e trimestralmente, respectivamente.

O "Cenário 6" traduz uma alteração física de um dos componentes da barreira de segurança, nomeadamente aquele cuja medida de importância do seu acontecimento básico de falha se destacou dos restantes acontecimentos, ou seja, a válvula à saída do colector de compressão. Desta forma, criaram-se condições para que haja uma indicação clara de que a válvula de seccionamento se encontra na posição de aberta no fim de cada intervenção ou teste efectuado. A solução encontrada passou por incluir esta verificação na Ordem de Trabalho (OT) de todas as intervenções, obrigando ainda a um procedimento de dupla verificação (reconhecido através de dois intervenientes distintos).

Muitos outros cenários poderiam ser retratados, ficando neste estudo apenas exemplificadas algumas situações para demonstração da sua potencialidade e exequibilidade. A Figura 6.12 mostra os vários Cenários equacionados anteriormente, mas de uma forma gráfica, para melhor visualização do que se pretende simular neste estudo.

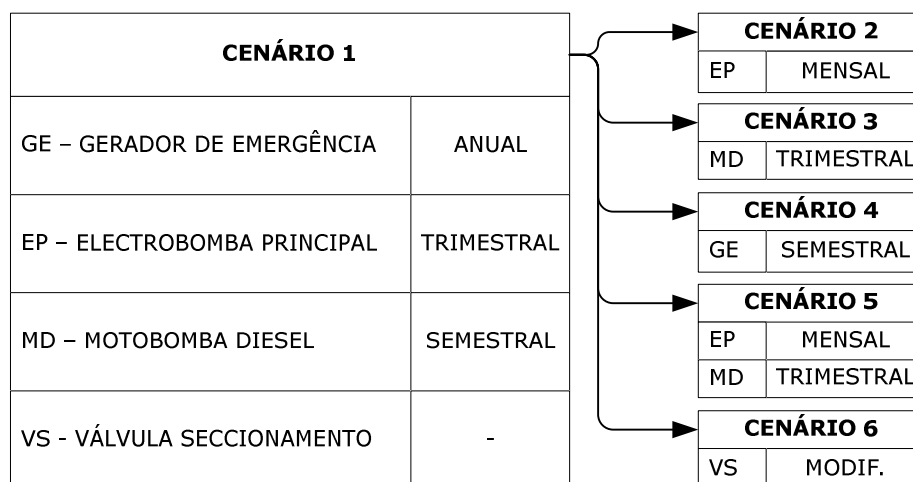



Figura 6.12 – Cenários alternativos

De referir que as taxas de avaria individuais associadas aos acontecimentos básicos poderiam eventualmente alterar-se face ao cenário inicial (Cenário 1), uma vez que as periodicidades para testes ou ensaios também se alteraram. No entanto, mantiveram-se os dados iniciais, por um lado por falta de dados credíveis relativos aos novos cenários, e por outro lado por os valores considerados serem de certa forma conservadores relativamente aos eventuais novos dados, uma vez que teoricamente as taxas de avaria seriam agora mais baixas em virtude de os períodos entre testes ou ensaios serem também mais apertados.

Introduzindo no modelo os novos cenários, reflexo das alterações anteriormente descritas, obtiveram-se os resultados apresentados na Tabela 6.10, correspondentes às indisponibilidades médias referentes ao acontecimento de topo.

Tabela 6.10 – *Indisponibilidades para Cenários alternativos*

Cenário#	Indisponibilidade média
Cenário 1	0,1497
Cenário 2	0,0534
Cenário 3	0,1340
Cenário 4	0,1496
Cenário 5	0,0475
Cenário 6	0,0684

Após uma breve análise aos resultados obtidos pode-se constatar que se obtém um ganho muito baixo em termos de disponibilidade quando se reduz a periodicidade dos testes ou ensaios da Motobomba Diesel de "Semestral" para "Trimestral" ou quando se reduz a periodicidade dos testes ou ensaios ao Gerador de Emergência de "Anual" para "Semestral".

Em contrapartida, a indisponibilidade da barreira de segurança é reduzida drasticamente quando se passam os testes ou ensaios da Electrobomba Principal de "Trimestral" para "Mensal" isoladamente ou em simultâneo com a alteração da periodicidade dos testes ou ensaios da Motobomba Diesel de "Semestral" para "Trimestral". Valores muito idênticos ao Cenário 5 são alcançados quando se promove a alteração à verificação da válvula de seccionamento à saída do colector de compressão (Cenário 6). A Figura 6.13 ilustra graficamente os vários cenários e as respectivas melhorias alcançadas.

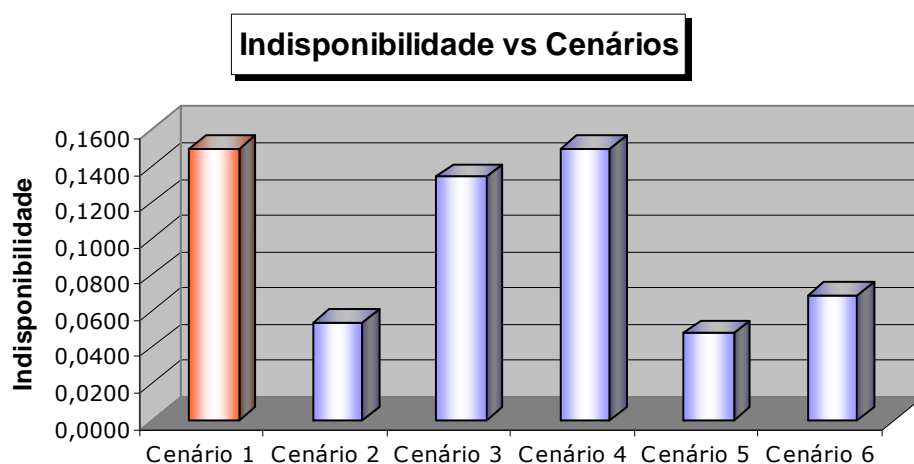



Figura 6.13 – Indisponibilidade vs Cenários

Desta forma, com as simples simulações efectuadas, ficamos com informação de uma forma quantificada quanto ao impacto que determinadas alterações podem ter na indisponibilidade da barreira de segurança em estudo. Assim, se os valores encontrados da indisponibilidade para os Cenários 2, 5 ou 6 forem toleráveis do ponto de vista do critério de aceitação estabelecido, caberá aos responsáveis pela gestão do risco e/ou manutenção decidir sobre qual a melhor opção a introduzir, apreciando aspectos como a viabilidade técnica e económica.

6.4 – Conclusões do Capítulo

No presente capítulo pretendeu-se dar seguimento à descrição teórica apresentada no Capítulo V, procedendo-se à aplicação da Metodologia RODS a uma barreira de segurança normalmente presente em qualquer instalação de risco elevado. O equipamento estudado foi uma Central de Bombagem de Água Contra Incêndio.

Efectuou-se uma apresentação detalhada deste tipo de sistemas, começando com uma perspectiva histórica, a justificação da sua necessidade e referindo alguns tipos de bombas e suas características principais.

Mostrou-se como são realizados os testes ou ensaios a este tipo de equipamentos, a sua importância no contexto da fiabilidade, assim como normas a seguir no seu procedimento. Explicou-se o princípio de funcionamento de uma Central de Bombagem

de Água Contra Incêndios. Referiu-se também que cerca de 35% das causas de falha neste tipo de equipamento se devem a alterações após comissionamento, às condições de exploração e aos procedimentos de manutenção aplicados durante o seu ciclo de vida.

Após a explicação detalhada de todos as características físicas e funcionais do equipamento passou-se ao estudo de um caso prático. Seguindo a Metodologia RODS, começou-se por definir a barreira de segurança, sua constituição e respectivas funções. De seguida identificaram-se os componentes de suporte (ou arranque), distinguindo-se os monitorizados dos não monitorizados. Quanto aos primeiros foi dada uma explicação sobre a razão da sua exclusão do estudo da primeira fase da Metodologia. No que respeita aos componentes de suporte não monitorizados, foram identificados os acontecimentos básicos que podem estar na origem das falhas, assim como definidas as periodicidades associadas a cada tipo de componentes.

Passou-se de seguida à construção da Árvore de Falhas, tendo em atenção a definição do acontecimento de topo, dos acontecimentos intermédios e de todos os acontecimentos básicos e a forma como este se relacionam, utilizando para o efeito portas lógicas estáticas. Foi justificada a não utilização de portas lógicas dinâmicas no presente modelo.

Seguiu-se depois uma análise qualitativa da Árvore de Falhas, com a determinação dos conjuntos de corte mínimos e sua interpretação baseada na ordem dos mesmos.

Considerando como parâmetros de entrada as taxas de avaria associadas a cada acontecimento básico e as periodicidades de inspecção, teste ou ensaio de cada sub-sistema funcional da Central de Bombagem procedeu-se à análise quantitativa da Árvore de Falhas. Desta forma foi possível determinar a indisponibilidade média associada ao acontecimento de topo (0,1497), assim como as indisponibilidades médias relativas a cada acontecimento intermédio e a cada acontecimento básico. Quanto a este aspecto, foi posteriormente realizada uma análise e interpretação dos resultados alcançados.

Para se perceber a influência de cada acontecimento básico no valor da indisponibilidade referente ao acontecimento de topo realizou-se uma análise das medidas de importância, usando a medida *Fussell-Vesely*. Desta forma foi possível verificar que um único acontecimento contribui em cerca de 70% para a ocorrência da falha no arranque da Central de Bombagem. Relativamente à Metodologia RAMS e tendo em conta os vários critérios de aceitação do risco é possível estipular se o valor alcançado como indisponibilidade é tolerável ou não.

Assumindo não aceitável o resultado da análise quantitativa, foram apresentados alguns cenários alternativos ao inicial, nomeadamente alterando algumas das periodicidades referentes à realização dos testes ou ensaios, ou procedendo a algumas modificações físicas ou funcionais dos componentes de suporte não monitorizados da barreira de segurança.

Desta forma, o capítulo termina com a simulação dos cenários alternativos e com o consequente cálculo da indisponibilidade média associada ao acontecimento de topo. Assim, chega-se à conclusão que realizando alguns testes ou ensaios com periodicidades mais apertadas que as do cenário inicial, se consegue um aumento da disponibilidade de 85% para cerca de 95,3%. Da mesma forma, recorrendo a uma simples modificação processual aquando da realização dos testes ou ensaios se consegue alcançar uma disponibilidade de cerca de 93,2%. Da interpretação das simulações realizadas também é possível verificar que em determinados casos não se ganha quase nada ao implementar certas alterações.

Considera-se importante e interessante a aplicação prática estudada neste capítulo, pois permite demonstrar a primeira fase da Metodologia RODS, assim como fazer referência a matérias descritas em capítulos anteriores como a Metodologia RAMS ou critérios de aceitação do risco.

CAPÍTULO VII

CONCLUSÕES E TRABALHOS FUTUROS

7.1 – Conclusões da Tese

O trabalho realizado pretende dar resposta ao objectivo proposto no Capítulo I, tendo sido desenvolvida toda a temática relativa a barreiras de segurança com base no enquadramento RAMS.

Para o efeito, foi proposta uma metodologia de análise a barreiras de segurança, tendo por base as particularidades e especificidades deste tipo de equipamentos, muitas vezes fulcrais para a salvaguarda da vida humana ou para a continuidade das actividades económicas.

Mostrou-se a importância das análises de risco realizadas em instalações industriais, e de como uma gestão cuidada das barreiras de segurança, através do conhecimento dos potenciais modos de falha e suas probabilidades de ocorrência, pode ser determinante. Saber a probabilidade de falha deste tipo de equipamentos sempre que são solicitados pode dar uma ideia concreta aos responsáveis pelas instalações do risco potencial, permitindo decidir sobre a sua aceitação.

Nessa vertente, foi abordado em particular o risco de incêndio, apresentando uma barreira de segurança considerada crucial para a diminuição ou mitigação das consequências deste tipo de fenómeno, nomeadamente uma Central de Bombagem de Água Contra Incêndios. Para essa barreira de segurança foi proposta uma metodologia de análise para a determinação da fiabilidade (Metodologia RODS), tendo por base a separação em duas fases funcionais, uma primeira referente à disponibilidade de

determinados componentes, designados componentes de suporte (ou arranque), e uma segunda fase relacionada com a fiabilidade dos componentes activos, permitindo aferir a probabilidade de continuidade do funcionamento durante uma determinada missão.

A grande preocupação prende-se com a primeira fase e com as chamadas "falhas ocultas", apenas teoricamente detectáveis aquando das intervenções periódicas realizadas no sentido de efectuar testes ou ensaios de funcionamento.

Mostrada a importância da primeira fase da metodologia, o estudo prosseguiu no sentido de testar a mesma através de uma aplicação prática. Dessa forma, estruturou-se uma Árvore de Falhas contendo os acontecimentos básicos relacionados com modos de falha dos componentes identificados como componentes de suporte não monitorizados, cuja ocorrência pode contribuir em maior ou menor escala para a ocorrência do acontecimento de topo.

Nesta fase, o conhecimento profundo do equipamento e das suas características funcionais mostra-se fundamental para se alcançarem resultados mais confiáveis. Trata-se de um tipo de equipamento que se encontra grande parte do seu ciclo de vida num estado "*dormant*", o que impossibilita a obtenção de uma quantidade significativa de dados de vida e o consequente tratamento através de metodologias tradicionais tendo em vista a obtenção de resultados fiabilísticos. Na fase de arranque determina-se a probabilidade de sucesso na transição do estado "*dormant*" para o estado de operação activa (correspondente à segunda fase da Metodologia RODS).

No presente trabalho foram introduzidas abordagens novas de construção de Árvores de Falhas, com recurso a portas lógicas dinâmicas. Pese embora o detalhe dado a estas novas ferramentas ao longo do texto, estabeleceu-se para a aplicação prática demonstrada uma estrutura apenas baseada em portas lógicas estáticas, simplificando a abordagem realizada. No entanto, ficam dadas as indicações sobre a sua aplicabilidade para outros trabalhos onde não seja possível restringir a Árvore de Falhas apenas a portas lógicas estáticas.

Devido à dificuldade em obter dados concretos, assumiram-se determinados pressupostos e estipularam-se valores relativos às taxas de avaria para cada acontecimento básico identificado. Muitos destes valores resultam mais da experiência dos fabricantes (e respectivas assistências técnicas) do que propriamente de uma recolha fidedigna de dados reais de um equipamento específico. Por outro lado, assente numa

base mais concreta e real, foram assumidas periodicidades individuais para a realização dos testes ou ensaios. Desta forma, foi possível seguir a metodologia estabelecida e efectuar uma análise qualitativa, seguida de uma análise quantitativa.

Na análise qualitativa foram determinados os conjuntos de corte mínimos (MCS), ou combinações de acontecimentos que levam à ocorrência do acontecimento de topo. Foi verificada a existência de um conjunto de primeira ordem, correspondendo a um erro humano que ocorre com alguma frequência. Esta é uma situação decorrente dos procedimentos de inspecção, teste ou ensaio e acontece quando inadvertidamente o técnico não procede à reabertura da referida válvula no fim da sua intervenção. Foram também identificadas outras situações correspondentes a conjuntos de corte de segunda ordem, merecendo a devida atenção por parte dos analistas.

Na sequência da análise quantitativa, e tendo em conta os dados de entrada do modelo (λ,τ), determinou-se a probabilidade referente à indisponibilidade associada ao acontecimento de topo, assim como as indisponibilidades individuais para os acontecimentos básicos e acontecimentos intermédios. Para o cenário inicialmente equacionado (Cenário 1), a indisponibilidade estimada referente à falha no arranque da central de bombagem de água contra incêndio é de 0,1497.

A influência ou contributo de cada acontecimento básico para o valor alcançado foi determinada através da realização de uma análise de sensibilidade, determinando-se assim as medidas de importância (*Importance Measures*), nomeadamente a medida *Fussell-Vesely*. Desta forma, foi possível confirmar que a indisponibilidade da válvula de seccionamento referida em parágrafos anteriores tem um peso de cerca de 70% da falha no arranque da central de bombagem.

Enquadrado na Metodologia RAMS e nos critérios de aceitação do risco, é possível decidir se o valor de indisponibilidade 0,1497 é tolerável ou não. Assumindo que o risco subjacente a esta indisponibilidade não é tolerável, procedeu-se à simulação de vários cenários alternativos, fazendo variar as periodicidades com que os testes ou ensaios são realizados ou alterando algumas lógicas no procedimento operacional das intervenções.

Desta simulação com cenários alternativos resultam distintas indisponibilidades associadas ao acontecimento de topo. Chega-se à conclusão que realizando alguns testes ou ensaios com periodicidades diferentes das inicialmente assumidas se consegue um aumento da disponibilidade de 85% para cerca de 95,3%. Da mesma forma, a alteração

introduzida ao nível operacional permite alcançar uma disponibilidade de cerca de 93,2%. Da interpretação das simulações realizadas também é possível verificar que em determinados casos não é compensatório estar-se a encurtar prazos para a realização dos testes ou ensaios.

Como conclusão final, é importante ressalvar a importância que assume este tipo de análises, uma vez que são efectuadas sobre equipamentos que ainda se encontram pouco explorados na óptica da fiabilidade, desconhecendo-se o seu comportamento quando são solicitados em situações reais de catástrofe.

7.2 – Trabalhos futuros

Em termos de estudos de fiabilidade, pode-se afirmar que até ao momento pouco existia sobre este tipo de barreiras de segurança. Com este trabalho espera-se ter dado um contributo importante para se perceberem alguns aspectos particulares destes equipamentos e assim mostrar algumas abordagens e metodologias passíveis de aplicação, no sentido de melhor se entender o risco potencial de uma instalação.

No seguimento do trabalho realizado, e como perspectivas de trabalhos futuros ficam por estudar algumas situações cujo desenvolvimento neste momento obrigaria o presente documento a tomar proporções volumosas e porventura estender-se no tempo indefinidamente.

No entanto, podem-se apontar alguns trabalhos futuros, nomeadamente consciencializar para esta problemática todos os que são responsáveis pela manutenção, pelo risco ou pela gestão dos activos, fomentando a implementação de procedimentos de monitorização deste tipo de barreiras, com o intuito de se adquirirem dados reais de taxas de avarias para determinadas situações de exploração e manutenção. Desta forma, poder-se-ia ultrapassar a dificuldade relatada e sentida durante a realização deste estudo.

Outro aspecto de grande relevo onde se poderia avançar mais um pouco e considerar como um factor extrínseco à barreira de segurança, é o estudo da fiabilidade humana e a relação Homem-máquina. De facto, é algo que pode ser determinante quando se calcula a disponibilidade ou fiabilidade de um equipamento desta natureza.

Pese embora tenha uma influência menor, para que a Metodologia RODS fosse completamente cumprida, seria necessário avançar-se com a segunda fase, verificando a fiabilidade dos componentes activos, e desta forma determinar-se a probabilidade de sucesso do sistema durante uma determinada missão. O cálculo da fiabilidade da barreira de segurança seria alcançado usando a probabilidade condicional, ou seja, calculando a probabilidade de sucesso para uma missão (segunda fase), dado o equipamento estar disponível quando solicitado (primeira fase).

REFERÊNCIAS

ADAMYAN, A. & HE, D. (2002), *Analysis of sequential failures for assessment of reliability and safety of manufacturing systems*, Reliability Engineering & System Safety, Vol. 76, pp. 227-236

AMARI, S., DILL, G. & HOWALD, E. (2003), *A New Approach to Solve Dynamic Fault Trees*, IEEE – Reliability and Maintainability Symposium, pp. 374-379

ANDREWS, J.D. & MOSS, T.R. (2002), *Reliability and Risk Assessment – Second Edition*, Professional Engineering Publishing Limited, ISBN 1.86058.290.7, London, UK

ANDREWS, J.D. & BARTLETT, L.M. (2005), *A branching search approach to safety system design optimisation*, Reliability Engineering & System Safety, Vol. 87, pp. 23-30

ANGADI, S.V., JACKSON, R.L., SHOE, S., FLOWERS, G.T, SUHLING, J.C., CHANG, Y., HAM, J. & BAE, J. (2009), *Reliability and life study of hydraulic solenoid valve – Part 2: Experimental study*, Engineering Failure Analysis, Vol. 16, pp. 944-963

ARNAULD, A. & NICOLE, P. (1996), *Logic or the Art of Thinking*, Cambridge University Press, ISBN 0-521-48249-6, London

ASSAF, T. & DUGAN, J.B. (2004), *Diagnostic Expert Systems from Dynamic Fault Trees*, Proceedings of the Annual Reliability and Maintainability Symposium, pp. 444-450

ASSIS, R. (2004), *Apoio à Decisão em Gestão da Manutenção – Fiabilidade e Manutenibilidade*, Lidel – Edições Técnicas, ISBN 972-757-298-7, Lisboa

ASSIS, R. (2010), *Apoio à Decisão em Manutenção na Gestão de Activos Físicos*, Lidel – Edições Técnicas, ISBN 978-972-757-605-0, Lisboa

BADÍA, F.G., BERRADE, M.D. & CAMPOS, C.A. (2002), *Optimal inspection and preventive maintenance of units with revealed and unrevealed failures*, Reliability Engineering & System Safety, Vol. 78, pp. 157-163

BAPTISTA, L.L. & DIAS, J.M. (2007), *A Manutenção Industrial numa Perspectiva RAM*, 9º Congresso Nacional de Manutenção, 22-23 de Novembro de 2007, Exponor, Porto.

BARROS, A., GRALL, A. & VASSEUR, D. (2009), *Estimation of common cause failure parameters with periodic tests*, Nuclear Engineering and Design, Vol. 239, pp. 761-768

BARTLETT, L.M., HURDLE, E.E. & KELLY, E.M. (2009), *Integrated system fault diagnostics utilising digraph and fault tree-based approaches*, Reliability Engineering & System Safety, Vol. 94, pp. 1104-1115

BOUDALI, H. & DUGAN, J.B. (2005), *A discrete-time Bayesian network reliability modeling and analysis framework*, Reliability Engineering & System Safety, Vol. 87, pp. 337-349

BURDEKIN, F.M. (2007), *General principles of the use of safety factors in design and assessment*, Engineering Failure Analysis, Vol. 14, pp. 420-433

BURROS, R.H. (1975), *Probability of failure of building from fire*, (Proc Am Soc Civ Eng), Journal of the Structural Division , Vol. 101, pp. 1947-1960

CARCHIA, M. (1999), *Non-Operating Reliability*, Carnegie Melon University [www.ece.cmu.edu/~koopman/des_s99/non_operating/]. Acedido em 12 de Fevereiro de 2009

CARINHAS, H. (2007), *Apontamentos de Fiabilidade*, Instituto Superior de Engenharia de Lisboa

CASTILLO, E., CONEJO, A., MINGUEZ, R. & CASTILLO, C. (2003), *An alternative approach for addressing the failure probability-safety factor method with sensitivity analysis*, Reliability Engineering & System Safety, Vol. 82, pp. 207-216

CEA 4001 (2009), *Sprinkler Systems: Planning and Installation*, Comité Européen des Assurances

CEPIN, M. & MAVKO, B. (2002), *A dynamic fault tree*, Reliability Engineering & System Safety, Vol. 75, pp. 83-91

CEPREVEN, RT2 ABA H2O (2006), *Regla Técnica Abastecimientos de Agua Contra Incêndios*, Asociación de Investigación para La Seguridad de Vidas y Bienes – Centro Nacional de Prevención de Danos y Pérdidas, ISBN 84-85597-91-5, Madrid

CHARRUAU, S., GUERIN, F., DOMINGUEZ, J. & BERTHON, J. (2006), *Reliability Estimation of Aeronautic Component by Accelerated Tests*, Microelectronics Reliability, Vol. 46, pp. 1451-1457

CHEW, S., DUNNETT, S. & ANDREWS, J.D. (2010), *Aircraft mission reliability modelling with maintenance free operating periods*, 38th ESReDA Seminar, Pécs, Hungary

CHING, J. (2009), *Equivalence between reliability and factor of safety*, Probabilistic Engineering Mechanics, Vol. 24, pp. 159-171

COLOMBO, S. & DEMICHELA, M. (2008), *The systematic integration of human factors into safety analysis: An integrating engineering approach*, Reliability Engineering & System Safety, Vol. 93, pp. 1911-1921

COULIBALY, A., HOUSSIN, R. & MUTEL, B. (2008), *Maintainability and safety indicators at design stage for mechanical products*, Computers in Industry, Vol. 59, pp. 438-449

COURTOIS, P. & DELSARTE, P. (2006), *On the optimal scheduling of periodic tests and maintenance for reliable redundant components*, Reliability Engineering & System Safety, Vol. 91, pp. 66-72

DELVOSALLE, C., FIÉVEZ, C., PIPART, A., FABREGA, J.C., PLANAS, E., CHRISTOU, M. & MUSHTAQ, F. (2005), *Identification of reference accident scenarios in SEVESO establishments*, Reliability Engineering System Safety, Vol. 90, pp. 238-246

DIANOUS, V. & FIÉVEZ, C. (2006), *ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance*, Journal of Hazardous Material, Vol. 130, pp. 220-233

DIEKEN, D. (2008), *Inspection, Testing and Maintenance of Fire Protection Systems at Electric Generating Plants*, Hartford Steam Boiler Inspection and Insurance Co. [www.hsb.com/thelocomotive/Story/FullStory/ST-FS-FIRESUP.html]. Acedido em 14 de Agosto de 2008

DIRECTIVA MÁQUINAS (1998), *On the approximation of the laws of the Member States related to machinery as amended by Directive 98/79/EC (Machinery Directive)*, EC, COUNCIL DIRECTIVE 98/37/EC

DIRECTIVA SEVESO, (1996), *On the control of major-accident hazards involving dangerous substances (Seveso II Directive)*, EC, COUNCIL DIRECTIVE 96/82/EC

DORP, J. & MAZZUCHI, T. (2005), *A general Bayes weibull inference model for accelerated life testing*, Reliability Engineering & System Safety, Vol. 90, pp. 140-147

DUIJM, N. & GOOSSENS, L. (2006), *Quantifying the influence of safety management on the reliability of safety barriers*, Journal of Hazardous Material, Vol. 130, pp. 284-292

DUIJM, N. (2008), *Safety-barriers diagrams as a safety management tool*, Reliability Engineering and System Safety, Vol. 94, pp. 332-341

DUTUIT, Y. & RAUZY, A. (1996), *A linear time Algorithm to find Modules of Fault Trees*, IEEE Trasactions on Reliability, Vol. 45, pp. 422-425

EN 12845:2004+A2:2009 (Ed) (2009), *Fixed firefighting systems. Automatic sprinklers systems. Design, installation and maintenance*, IPQ

ETI, M.C., OGAJI, S.O.T. & PROBERT, S.D. (2007), *Integrating reliability, availability, maintainability and supportability with risk analysis for improved operation of the Afam thermal power-station*, Applied Energy, Vol. 84, pp. 202-221

FARD, N. & LI, C. (2009), *Optimal simple step stress accelerated life test design for reliability prediction*, Journal of Statistical Planning and Inference, Vol. 139, pp. 1799-1808

FERNANDEZ, P. (1996), *Probabilistic fire analysis capabilities, applications and weak points*, Nuclear Engineering and Design, Vol. 167, pp. 77-83

FERREIRA, L.A. (1998), *Uma Introdução à Manutenção*, Publindústria, ISBN 972-95794-4-X, Porto

FONTANA, M., FAVRE, J.P. & FETZ, C. (1999), *A survey of 40.000 building fires in Switzerland*, Fire Safety Journal, Vol. 32, pp. 137-158

FREITAG, S., BEER, M., GRAF, W. & KALISKE, M. (2009), *Lifetime prediction using accelerated test data and neural networks*, Computers and Structures, Vol. 87, pp. 1187-1194

GALILEO® v3.0 (2004), *Dynamic Fault Tree Analysis Tool*, Exelix, University of Virginia, USA

GARCÍA-GARCÍA, P., LÓPEZ-LÓPEZ, A. & FERNÁNDEZ, A.G. (2008), *Study of the shelf life of ripe olives using an accelerated test approach*, Journal of Food Engineering, Vol. 84, pp. 569-575

GOWLAND, R. (2006), *The accidental risk assessment methodology for industries (ARAMIS) / layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?*, Journal of Hazardous Materials, Vol. 130, pp. 307-310

GULATI, R. & DUGAN, J.B. (1997), *A modular approach for analyzing static and dynamic fault trees*, Reliability and Maintainability Symposium, pp. 57-63

GUO, H. & YANG, X. (2008), *Automatic creation of Markov models for reliability assessment of safety instrumented systems*, Reliability Engineering & System Safety, Vol. 93, pp. 807-815

HARRIS, A.P. (1980), *Reliability in the dormant condition*. Microelectronics and Reliability. Vol. 20, pp. 33-44

HAUPTMANNS, U. (2008), *The impact of reliability data on probabilistic safety calculations*, Journal of Loss Prevention in the Process Industries, Vol. 21, pp. 38-49

HAUPTMANNS, U. (2009), *Different sets of reliability data and success criteria in a probabilistic safety assessment for a plant producing nitroglycol*, Journal of Hazardous Materials, Vol. 162, pp. 1322-1329

HAUPTMANNS, U., MARX, M. & GRUNBECK, S. (2008), *Availability analysis for a fixed wet sprinkler system*, Fire Safety Journal, Vol. 43, pp. 468-476

HENLEY, E. & KUMAMOTO, H. (1981), *Reliability Engineering and Risk Assessment*, Prentice-Hall, Inc., ISBN 0-13-772251-6, New Jersey, USA

HERDER, P.M., LUIJK, J.A. & BRUIJNOOGE, J. (2008), *Industrial application of RAM modelling - Development and implementation of a RAM simulation model for the Lexan plant at GE industrial, Plastics*, Reliability Engineering & System Safety, Vol. 93, pp. 501-508

HOKSTAD, P. & FROVIG, A. (1996), *The modelling of degraded and critical failures for components with dormant failures*, Reliability Engineering & System Safety, Vol. 51, pp. 189-199

HOLLNAGEL, E. (1998), *The State of Human Reliability Analysis, Cognitive Reliability and Error Analysis Method (CREAM)*, Elsevier, ISBN 978-0-08-042848-2, Amsterdam

HOLLNAGEL, E. (2004), *Barrier and acident prevention*, Ashgate Publishing Limited, ISBN 0-7546-4301-8, Hampshire, UK

HOLLNAGEL, E. (2008), *Risk + barriers = safety?*, Safety Science, Vol. 46, pp. 221-229

HOSTIKKA, S. & KESKI-RAHKONEN, O. (2003), *Probabilistic simulation of fire scenarios*, Nuclear Engineering and Design, Vol. 224, pp. 301-311

HUGHES, G. & KORNOWA-WEICHEL, M. (2004), *Whose fault is it anyway? A practical illustration of human factors in process safety*, Journal of Hazardous Materials, Vol. 115, pp. 127-132

HURDLE, E.E., BARTLETT, L.M. & ANDREWS, J.D. (2007), *System fault diagnostics using fault tree analysis*, Journal of Risk and Reliability, Part O (Proceedings of the IMechE), Vol. 221(1), pp. 43-55

IEC 60300-3-9 (1995), *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*, International Electrotechnical Comission, Geneva, Switzerland

IEC:61508 – Part 1-7 (1998), *Functional Safety of electrical / electronic / programmable electronic safety-related systems*, International Electrotechnical Commission, Geneva, Switzerland

IEC:61511 – Part 1-7 (2002), *Functional Safety – Safety instrumented systems for the process industry sector*, International Electrotechnical Commission, Geneva, Switzerland

ISOGRAPH® (1999), *Reliability Workbench Version 7.0* – User Manual (Item)

ITO, K. & NAKAGAWA, T. (2000), *Optimal Inspection Policies for a Storage System with Degradation at Periodic Tests*, Mathematical and Computer Modelling, Vol. 31, pp. 191-195

IVERSON, D. & PATTERSINE-HINE, F. (1995), *Advances in digraph model processing applied to automated monitoring and diagnosis*, Reliability Engineering & System Safety, Vol. 49(3), pp. 325-334

JACKSON, Y., TABBAGH, P., GIBSON, P. & SEGLIE, E. (2005), *The New Department of Defense (DoD) Guide for Achieving and Assessing RAM*, RAMS 2005

JOHANSSON, H. (2001), *Decision Making in Fire Risk Management*, Report 1022, Lund University, Department of Fire Safety Engineering, Lund, Sweden

KANG, D.I., HWANG, M.J. & HAN, S.H. (2009), *Estimation of the common cause failure probabilities of the components under mixed testing schemes*, Annals of Nuclear Energy, Vol. 36, pp. 493-497

KECECIOGLU, D. (2002), *Reliability Engineering Handbook - Vol 1*, Department of Aerospace and Mechanical Engineering – The University of Arizona, DEStech Publications, ISBN 1-932078-00-2, Pennsylvania

KECKLUND, L., EDLAND, A., WEDIN, P. &SVENSON, O. (1996), *Safety barrier function analysis in a process industry: A nuclear power application*, International Journal of Industrial Ergonomics, Vol. 17, pp. 275-284

KEREN, N., WEST, H.H., ROGERS, W.J., GUPTA, J.P. & MANNAN, M.S. (2003), *Use of failure rate databases and process safety performance measurements to improve process safety*, Journal of Hazardous Materials, Vol. 104, pp. 75-93

KHATIBI, G., WROCZEWSKI, W., WEISS, B. & LICHT, T. (2008), *A fast mechanical test technique for life time estimation of micro-joints*, Microelectronics Reliability, Vol. 48, pp. 1822-1830

KIM, T., KIM, J., KIM, Y. & KIM, K. (2002), *Current risk management status of the Korean petrochemical industry*, Journal of Loss Prevention in the Process Industries, Vol. 15, pp. 311-318

KJELLÉN, U. (2000), *Prevention of accidents through experience feedback*, Taylor & Francis, London

KNEGTERING, B. & BROMBACHER, A.C. (2000), *A method to prevent excessive numbers of Markov states in Markov models for quantitative safety and reliability*, ISA Transactions, Vol. 39, pp. 363-369

KOSAKI, A. (2008), *Evaluation method of corrosion lifetime of conventional stainless steel canister under oceanic air environment*, Nuclear Engineering and Design, Vol. 238, pp. 1233-1240

KUMAMOTO, H. (2007), *Satisfying Safety Goals by Probabilistic Risk Assessment*, Springer Series in Reliability Engineering, ISBN 978-1-84628-681-0, Springer-Verlag London Limited

KUMAR, C.S., ARUL, A.J., SINGH, O.P. & RAO, K.S. (2005), *Reliability analysis of shutdown system*, Annals of Nuclear Energy, Vol. 32, pp. 63-87

LEWIS, S.M. (2006), *NFPA Journal Latinoamericano*, Junho 2006, pp. 14-17

LIE, T.T. (1998), *Optimal fire resistance of structures*, (Proc Am Soc Civ Eng) Journal of the Structural Division, Vol. 98, pp. 215-232

LIN, Y. (2005), *Estimations of the probability of fire occurrences in buildings*, Fire Safety Journal, Vol. 40, pp. 728-735

LONG, W., SATO, Y. & HORIGOME, M. (2000), *Quantification of sequential failure logic for fault tree analysis*, Reliability Engineering & System Safety, Vol. 67, pp. 269-274

LUNDTEIGEN, M.A. & RAUSAND, M. (2007), *Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing*, Journal of Loss Prevention in the Process Industries, Vol. 20, pp. 218-229

MANIAN, R., COPPIT, D.W., SULLIVAN, K.J. & DUGAN, J.B. (1999), *Bridging the gap between Fault Tree Analysis Modeling Tools and the Systems being Modeled*, Proceedings of the 1999 Reliability and Maintainability Symposium, pp. 105-111

MARSEGUERRA, M., ZIO, E. & MARTORELL, S. (2006), *Basics of genetic algorithms optimization for RAMS applications*, Reliability Engineering & System Safety, Vol. 91, pp. 977-991

MARTINEZ, E. (1984), *Storage Reliability with Periodic Test*, Proceedings of Annual Reliability and Maintainability Symposium, pp. 181-185

MARTORELL, S., VILLANUEVA, J.F., CARLOS, S., NEBOT, Y., SÁNCHEZ, A., PITARCH, J.L. & SERRADELL, V. (2005), *RAMS+C informed decision-making with application to multi-objective optimization of technical specifications and maintenance using genetic algorithms*, Reliability Engineering & System Safety, Vol. 87, pp. 65-75

MARTORELL, S., SANCHEZ, A. & CARLOS, S. (2007), *A tolerance interval based approach to address uncertainty for RAMS+C optimization*, Reliability Engineering & System Safety, Vol. 92, pp. 408-422

MESHKAT, L., DUGAN, J. & ANDREWS, J.D. (2000), *Analysis of safety systems with on-demand and dynamic failure modes*, *iodic Test*, Proceedings of Annual Reliability and Maintainability Symposium, pp. 14-21

MIL-HDBK-217F (1991), *Reliability Prediction of Electronic Equipment*, United States of America, DoD -Department of Defense

MIL-STD 882-C (1993), *System Safety Program Requirements*, Military Standard, United States of America, DoD - Department of Defense

MONCHY, F. (1996), *La Fonction Maintenance – Formation à la gestion de la maintenance industrielle*, Masson, ISBN 2-225-85518-8, Paris

MONCHY, F. (2003), *Maintenance – Méthodes et organisations – 2e édition*, Série Gestion Industrielle, L'Usine Nouvélle, Dunod, ISBN 2-10-007816-X, Paris

MOTTA, S. & COLOSIMO, E. (2002), *Determination of preventive maintenance periodicities of standby devices*, Reliability Engineering & System Safety, Vol. 76, pp. 149-154

MOUBRAY, J. (1997), *Reliability-Centered Maintenance (RCM) – Second Edition*, Industrial Press, Inc., ISBN 0-8311-3146-2, Oxford, Great Britain

NAKADA, M. & MIYANO, Y. (2009), *Accelerated testing for long-term fatigue strength of various FRP laminates for marine use*, Composites Science and Technology, Vol. 69, pp. 805-813

NEOGY, P. et al (1996), *Hazard and barrier analysis guidance document – Rev. 0*, US Department of Energy (DoE), EH-33 Office of Operating Experience Analysis and Feedback [http://mentalmodels.mitre.org/cog_eng/reference_documents/hazard%20and%20barrier%20analysis%20guide.pdf]. Acedido em 11 de Junho de 2009

NFPA 20 (2003), *Standard for the Installation of Stationary Pumps for Fire Protection*, National Fire Protection Association, USA

NFPA 25 (2002), *Inspection, Testing and Maintenance of Water-Based Fire Protection Systems*, National Fire Protection Association, USA

NOLAN, D. (1998), *Fire Fighting Pumping System at Industrial Facilities*, Noyes Publications, ISBN 0-8155-1428-X, New Jersey, U.S.A.

NP EN 13306 (2007), *Terminologia da Manutenção*, IPQ, Almada

NP EN 50126 (2000), *Aplicações Ferroviárias – Especificação e demonstração de Fiabilidade, Disponibilidade, Manutibilidade e Segurança (RAMS)*, IPQ, Almada

NS 5814 (1991), *Hazard Analysis, Guidance to NS (Norwegian Standard) 5814*, SINTEF

NS Z-013 (2001), *Risk and emergency preparedness analysis - Norsok Standard, Rev. 2*, Norwegian Technology Centre, Oslo, Norway

NSWC-09 (2009), *Handbook of Reliability Prediction Procedures for Mechanical Equipment*, Logistics Technology Support, Naval Surface Warfare Center – Carderock Division

O'CONNOR, P.D.T. (1999), *Practical Reliability Engineering – 3rd Edition Revised*, John Wiley & Sons, Ltd., ISBN 0-471-95767-4, Chichester, England

ORBECK, T. (1990), *Fire Hazards – Present Codes and Standards*, Dow Corning Corp., IEEE Electric Insulation Magazine, Vol. 6, pp. 8-11

OREDA (2002), *Offshore Reliability Data – 4th Edition*, Prepared by SINTEF Industrial Management, Published by the OREDA Participants

OU, Y. & DUGAN, J.B. (2000), *Sensitivity Analysis of Modular Dynamic Fault Trees*, Proceedings of IEEE International Computer Performance and Dependability Symposium, pp. 35-43

OZSOY, S., CELIK, M. & KADIOGLU, F.S. (2008), *An accelerated life test approach for aerospace structural components*, Engineering Failure Analysis, Vol. 15, pp. 946-957

PALLEROSI, C. (2006), *Confiabilidade, a Quarta Dimensão da Qualidade – Conceitos Básicos e Métodos de Cálculo (Volume 1)*, Reliasoft Brasil

PALLEROSI, C. (2007), *Confiabilidade, A Quarta Dimensão da Qualidade - Confiabilidade Humana – Volume 10*, ReliaSoft Brasil

PALLEROSI, C. (2007b), *Confiabilidade, a Quarta Dimensão da Qualidade – Confiabilidade de Sistemas (Volume 4)*, Reliasoft Brasil

PALLEROSI, C. (2007c), *Confiabilidade, a Quarta Dimensão da Qualidade – Ensaios Acelerados (Volume 3)*, Reliasoft Brasil

PALLEROSI, C. (2007d), *Confiabilidade, a Quarta Dimensão da Qualidade – Mantenabilidade e Disponibilidade (Volume 5)*, Reliasoft Brasil

PECHT, J. & PECHT, M. (1995), *Long term non-operating reliability of electronic products*, CRC Press, ISBN 0-8493-9621-2, Boca Raton, USA

PEI, P., CHANG, Q. & TANG, T. (2008), *A quick evaluating method for automotive fuel cell lifetime*, International Journal of Hydrogen Energy, Vol. 33, pp. 3829-3836

PEREIRA, F.J.D. (1996), *Modelos de Fiabilidade em Equipamentos Mecânicos*, Tese de Doutoramento, Faculdade de Engenharia da Universidade do Porto, Porto

PETROLEUM SAFETY AUTHORITY (2002), *Guidelines to regulations relating to management in the petroleum activities (The Management Regulations)*, Stavanger, Norway

PLACEK, V., KOHOUT, T., HNÁT, V. & BARTONICEK, B. (2009), *Assessment of the EPDM seal lifetime in nuclear power plants*, Polymer Testing, Vol. 28, pp. 209-214

RAHIKAINEN, J. & KESKI-RAHKONEN, O. (2004), *Statistical determination of ignition frequency of structural fires in different premises in Finland*, Fire Technology, Vol. 40, pp. 335-353

RAJPAL, P.S., SHISODIA, K.S. & SEKHON, G.S. (2006), *An artificial neural network for modelling reliability, availability and maintainability of a repairable system*, Reliability Engineering & System Safety, Vol. 91, pp. 809-819

RAMACHANDRAN, G. (1980), *Statistical methods in risk evaluation*, Fire Safety Journal, Vol. 2, pp. 125-145

RAMACHANDRAN, G. (1999), *Fire safety management and risk assessment*, MCB University Press, Vol. 17, Number 9/10, pp. 363-376

RAMIREZ-MARQUEZ, J.E. & COIT, D.W. (2007), *Optimization of system reliability in the presence of common cause failures*, Reliability Engineering & System Safety, Vol. 92, pp. 1421-1434

RAUSAND, M. & HOYLAND, A. (2004), *System Reliability Theory; Models, Statistical Methods and Applications (Second Edition)*, Wiley, ISBN 0-471-47133-X, New York

REASON, J. (1990), *Human Error*, Cambridge University Press, ISBN 0-521-31419-4, Cambridge, United Kingdom

RELEX 2009® v11.0 (2009), Relex Software Corporation, PTC InSight Product, USA

ROUVROYE, J.L. & BLIECK, E.G. (2002), *Comparing safety analysis techniques*, Reliability Engineering & System Safety, Vol. 75, pp. 289-294

RUTSTEIN, R. & CLARKE, M.B.J. (1979), *The probability of fire in different sectors of industry*, Fire Surveyor, Vol. 20, pp. 3

SCHNEEWEISS, W. (1999), *The Fault Tree Method (in the Fields of Reliability and Safety Technology)*, LiLoLe-Verlag GmbH (publ. Co. Ltd.), ISBN 3-934447-01-5, Hagen, Germany

SCHNEEWEISS, W. (2004), *Petri Net Picture Book*, LiLoLe-Verlag GmbH (publ. Co. Ltd.), ISBN 3-934447-08-2, Hagen, Germany

SEMAN, ETZL & PURNELL (1988), *Reliability, Maintainability, Testability, Design for Dormancy – RADC-TR-88-110 Final Technical Report*, Lockheed Electronics Company, Inc, Rome Air Development Center, New York

SHALEV, D.M. & TIRAN, J. (2007), *Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations*, Reliability Engineering & System Safety, Vol. 92, pp. 1231-1241

SHALUF, I., AHMADUN, F. & SAID, A. (2003), *Fire incident at a refinery in West Malaysia: the causes and lessons learned*, Journal of Loss Prevention in the Process Industries, Vol. 16, pp. 297-303

SHARMA, R.K. & KUMAR, S. (2008), *Performance modelling in critical engineering systems using RAM analysis*, Reliability Engineering & System Safety, Vol. 93, pp. 891-897

SINNAMOM, R.M. & ANDREWS, J.D. (1997), *New approaches to evaluating fault trees*, Reliability Engineering & System Safety, Vol. 58, pp. 89-96

SIU, N., KARYDAS, D. & TEMPLE, J. (1990), *Bayesian assessment of modelling uncertainties: application to fire risk assessment*, Massachusetts Institute of Technology, Factory Mutual Research Corp., International Symposium on Uncertainty Modeling and Analysis, pp. 579-584

SKLET, S. (2006), *Safety barriers: Definition, classification, and performance*, Journal of Loss Prevention in the Process Industries, Vol. 19, pp. 494-506

SOBRAL, J. (2003), *Análise RAMS de Sistemas de Combate a Incêndio em Edifícios Públicos*, Tese de Mestrado, FEUP, Porto

SORENSEN, J.N. (2002), *Safety culture: a survey of the state-of-the-art*, Reliability Engineering & System Safety, Vol. 76, pp. 189-204

SUN, H. & ANDREWS, J.D. (2004), *Identification of independent modules in fault trees which contain dependent basic events*, Reliability Engineering & System Safety, Vol. 86, pp. 285-296

SVENSON, O. (1991), *The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries*, Risk Analysis, Vol. 11, pp. 499-507

TELCORDIA SR-332 (Bellcore TR-332) (2006), *Reliability Prediction Procedure for Electronic Equipment*, US Commercial Telecommunication Standard

THE ROME LABORATORY (1993), *Reliability Engineer's Toolkit – An Application Oriented Guide for the Practicing Reliability Engineer*, Systems Reliability Division – Rome Laboratory, Air Force Material Command (AFMC), New York

TILLANDER, K. (2004), *Utilisation of statistics to assess fire risks in buildings*, Espoo, VTT Publications 537.224 p. + app. 37 p.

TIXIER, J., DUSSERRE, G., SALVI, O. & GASTON, D. (2002), *Review of 62 risk analysis methodologies of industrial plants*, Journal of Loss Prevention in the Process Industries, Vol. 15, pp. 291-303

TORRES-ECHEVERRÍA, MARTORELL, S. & THOMSON, H.A. (2009), *Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy*, Reliability Engineering & System Safety, Vol. 94, pp. 162-179

U.S. NUCLEAR REGULATORY COMMISSION (1981), *Fault Tree Handbook*, NUREG-0492, Washington

VALENTINE, V. & ISMAN, K. (2006), *Bombas para Sistemas com Sprinklers* (Artigo publicado no "Manual de Engenharia Segurança Contra Incêndios"), ISBN 972-99554-1-7, Bombas Grundfos Portugal

VAURIO, J.K. (2001), *Fault tree analysis of phased mission systems with repairable and non-repairable components*, Reliability Engineering & System Safety, Vol. 74, pp. 169-180

VAURIO, J.K. (2002), *Extensions of the uncertainty quantification of common cause failure rates*, Reliability Engineering & System Safety, Vol. 78, pp. 63-69

VAURIO, J.K. (2003), *Common cause failure probabilities in standby safety system fault tree analysis with testing – scheme and time dependencies*, Reliability Engineering & System Safety, Vol. 79, pp. 43-57

VAURIO, J.K. (2005), *Uncertainties and quantification of common cause failure rates and probabilities for system analyses*, Reliability Engineering & System Safety, Vol. 90, pp. 186-195

VAURIO, J.K. (2007), *Consistent mapping of common cause failure rates and alpha factors*, Reliability Engineering & System Safety, Vol. 92, pp. 628-645

VIEGAS, D. (2006), *Perspectiva Histórica da Luta do Homem Contra o Fogo* (Artigo publicado no "Manual de Engenharia Segurança Contra Incêndios"), ISBN 972-99554-1-7, Bombas Grundfos Portugal

VOLKANOVSKI, A., CEPIN, M. & MAVKO, B. (2009), *Application of the fault tree analysis for assessment of the power system reliability*, Reliability Engineering & System Safety, Vol. 94, pp. 1116-1127

WANG, S., JI, Y., DONG, W. & YANG, S. (2007), *Design and RAMS Analysis of a Fault-Tolerant Computer Control System*, Tsinghua Science and Technology, ISSN 1007-0214 21/49, Vol. 12, Number S1, pp. 116-121

WU, S. & CLEMENTS-CROOME, D. (2007), *Burn-in policies for products having dormant states*, Reliability Engineering & System Safety, Vol. 92, pp. 278-285

WU, S. & LI, H. (2007), *Warranty cost analysis for products with a dormant state*, European Journal of Operational Research, Vol. 182, pp. 1285-1293

YEO, I., SUH, Y. & MUN, S. (2008), *Development of a remaining fatigue life model for asphalt black base through accelerated pavement testing*, Construction and Building Materials, Vol. 22, pp. 1881-1886

ZANG, T., XIE, M. & HORIGOME, M. (2006), *Availability and reliability of k-out-of-(M+N):G warm standby systems*, Reliability Engineering & System Safety, Vol. 91, pp. 381-387

ZIO, E. (2007), *An Introduction to the Basics of Reliability and Risk Analysis*, Series in Quality, Reliability and Engineering Statistics – Vol. 13, World Scientific Publishing Co. Pte. Ltd., ISBN-13 978-981-270-639-3, Singapore

ZIO, E. (2009), *Computational Methods for Reliability and Risk Analysis*, Series in Quality, Reliability and Engineering Statistics – Vol. 14, World Scientific Publishing Co. Pte. Ltd., ISBN-13 978-981-283-901-5, Singapore

ANEXO I

DISTRIBUIÇÕES ESTATÍSTICAS

A1 – Distribuições Estatísticas

A1.1 – Distribuição de Weibull

A distribuição de Weibull é uma das mais utilizadas devido à sua versatilidade, adaptando-se à maioria dos casos práticos referentes a componentes, com razoável precisão. Permite caracterizar as avarias durante os três períodos característicos da vida de um bem típico (início da vida operacional, vida útil e desgaste), onde a taxa de avarias é decrescente na primeira, constante na segunda e crescente na última. Esta distribuição pode apresentar-se em três formas: tri-paramétrica, bi-paramétrica e mono-paramétrica.

A influência de cada um dos seus parâmetros na fiabilidade do bem pode ser estudada mais em pormenor, quando tal se justifique. Outros tipos de distribuições, como a Exponencial, a Normal e a Lognormal acabam por ser casos particulares da distribuição de Weibull.

Distribuição de Weibull tri-paramétrica

Na sua forma tri-paramétrica, a função densidade de probabilidade de falha é expressa por:

$$f(t) = \frac{\beta}{\eta} \cdot \left(\frac{t-\gamma}{\eta} \right)^{\beta-1} \cdot e^{-\left(\frac{t-\gamma}{\eta} \right)^{\beta}} \qquad \text{(A1.1)}$$

onde:

t = Variável referida à grandeza, mensurável, que mede a extensão da utilização do bem (tempo, número de ciclos, operações, distância percorrida, etc…)

γ = Parâmetro de posição ou vida inicial (pode ser negativo, nulo ou positivo);

β = Parâmetro de forma, que define a variação da fiabilidade ao longo da vida do bem;

η = Parâmetro de escala ou vida característica, referida a $R=e^{-1}$ ou $R=0,367879$ ($\eta=1/\lambda_0$)

A Figura A1.1 mostra a função densidade de probabilidade de falha para a Distribuição de Weibull (tri-paramétrica), de acordo com vários valores do Parâmetro de Forma (β).

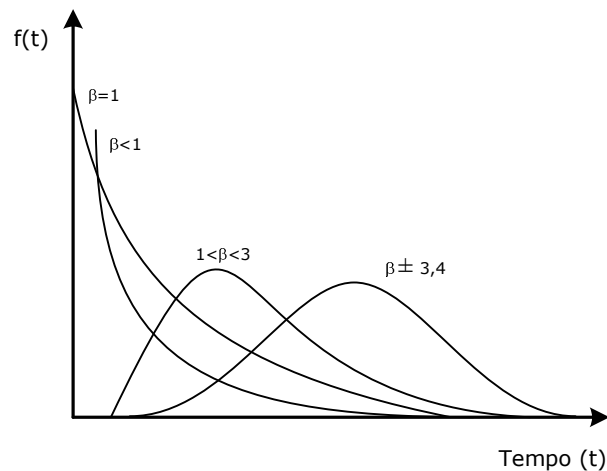



Figura A1.1 – Função densidade de probabilidade para a Distribuição de Weibull tri-paramétrica

Tendo em conta a expressão (2.5), a equação que permite o cálculo da fiabilidade para a Distribuição de Weibull tri-paramétrica é dada por:

$$R(t) = e^{-\left[\left(\frac{t-\gamma}{\eta} \right) \right]^{\beta}} \qquad \text{(A1.2)}$$

Distribuição de Weibull bi-paramétrica

A forma bi-paramétrica resulta do exemplo anterior quando o parâmetro de posição (γ) é nulo. Normalmente corresponde a bens novos, sem vida inicial[25].

Assim, a função densidade de probabilidade de falha é caracterizada pela seguinte expressão:

$$f(t) = \frac{\beta}{\eta}.\left(\frac{t}{\eta}\right)^{\beta-1}.e^{-\left(\frac{t}{\eta}\right)^{\beta}} \quad \text{(A1.3)}$$

E a consequente equação da fiabilidade dada por:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} \quad \text{(A1.4)}$$

Distribuição de Weibull mono-paramétrica (exponencial)

A distribuição de Weibull torna-se mono-paramétrica se, além de ter um parâmetro de posição nulo, também o seu parâmetro de forma (β) assume o valor unitário (1), o que significa possuir uma taxa de avarias constante ($\lambda_0=\lambda$), e daí podermos afirmar que se trata de uma distribuição semelhante à convencional distribuição exponencial. A função densidade de probabilidade de falha é dada por:

$$f(t) = \frac{1}{\eta}.e^{-\left(\frac{t}{\eta}\right)} = \lambda.e^{-\lambda.t} \quad \text{(A1.5)}$$

E a função de fiabilidade virá definida por:

$$R(t) = e^{-\lambda.t} = e^{-\left(\frac{t}{\eta}\right)} \quad \text{(A1.6)}$$

[25] A noção de ausência de vida inicial corresponde à situação em que não há um período inicial bem definido antes do qual não se podem verificar falhas.

A1.2 – Distribuição Normal

Um bem cujos dados referentes aos tempos de ocorrência de avaria se ajustem a uma distribuição normal significa que existe um valor médio (μ) para o tempo de avaria, em relação ao qual a distribuição é simétrica. Significa também que existem poucas avarias no início e no fim dos tempos de vida do bem.

O segundo parâmetro da distribuição é o desvio padrão (σ). Quanto menor for, maiores são os períodos inicial final de vida desse bem com poucas avarias. Na distribuição Normal, o valor médio (média) coincide com a mediana e com a moda. A distribuição Normal é característica de bens que apresentam um valor médio para a avaria bem definido e onde as avarias se distribuem de forma simétrica em torno desse valor, como é o caso das baterias de automóveis, escovas de motores eléctricos, pneus, lâmpadas, etc…). Este tipo de distribuição ajusta-se à maior parte dos casos de componentes cujo modo de falha principal está relacionado com a degradação característica de alguns componentes com a idade. Uma variável aleatória – seja o tempo de avaria "t" - é normalmente distribuída quando a sua função densidade de probabilidade de falha obedece à seguinte expressão:

$$f(t) = \frac{1}{\sigma.\sqrt{2.\pi}}.e^{-\frac{1}{2}.\left[\frac{(t-\mu)}{\sigma}\right]^2} \qquad \text{(A1.7)}$$

onde:

μ = Valor médio dos tempos até à avaria;

σ = Desvio padrão dos tempos até à avaria.

A função densidade de probabilidade referente à Distribuição Normal pode ser representada graficamente, conforme Figura A1.2, onde se pode verificar a influência da média (μ) - Figura A1.2(a) e a influência do desvio-padrão (σ) – Figura A1.2(b).

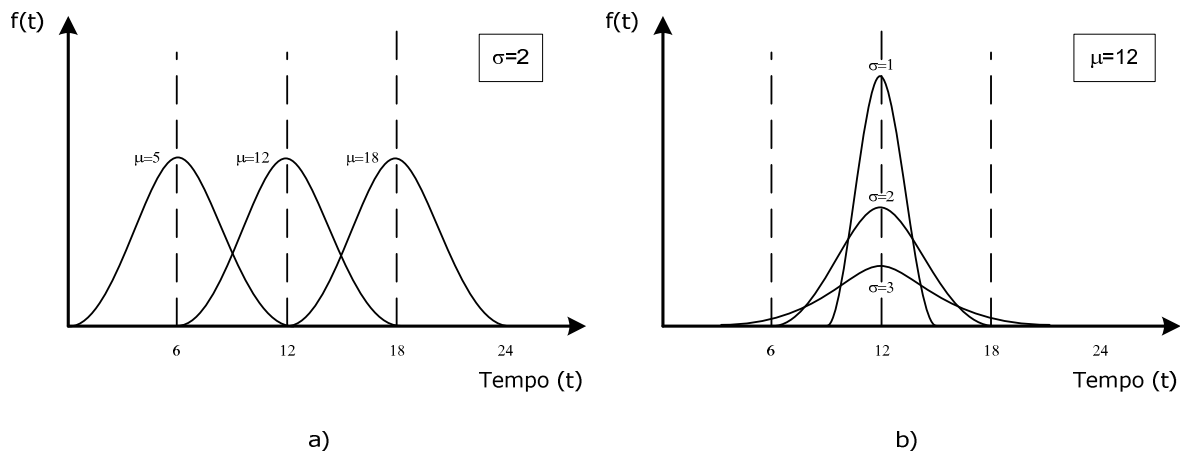



Figura A1.2 – Função densidade de probabilidade para a distribuição Normal

Normalmente, para comodidade do cálculo da probabilidade acumulada de falha "F(t)", transforma-se a variável "t" adimensional e representa-se a distribuição Normal de forma padronizada (standardizada) pela variável "z", que tem média igual a zero (μ=0) e desvio padrão igual a um (σ=1). Os valores de "z" podem então ser analisados em tabelas da distribuição Normal (ver **Anexo II**), determinando-se a probabilidade acumulada de falha. O cálculo da fiabilidade pode ser obtido por:

$$R(t) = \int_{t}^{\infty} \frac{1}{\sigma.\sqrt{2.\pi}} .e^{-\frac{1}{2}.\left[\frac{(t-\mu)}{\sigma}\right]^2} .dt \qquad \text{(A1.8)}$$

De salientar que esta expressão não possui uma solução directa, podendo ser calculada através de tabelas obtidas por cálculo numérico, ou por comodidade com recurso a programas informáticos específicos.

A1.3 – Distribuição Lognormal

Uma variável aleatória (t) é Lognormalmente distribuída se o seu logaritmo natural ou nepperiano (t'=ln t) é normalmente distribuído. Trata-se de uma distribuição assimétrica, tendendo para uma simetria para baixos valores de desvio padrão. As principais aplicações práticas correspondentes a esta distribuição são as avarias de rolamentos, motores eléctricos, geradores eléctricos, isoladores eléctricos, etc. De uma forma geral, este tipo de distribuição ajusta-se à maior parte dos casos de bens cujo modo de falha

principal está relacionado com a fadiga. A função densidade de probabilidade de falha para a distribuição Lognormal é dada por:

$$f(t') = \frac{1}{\sigma'.\sqrt{2.\pi}}.e^{-\frac{1}{2}.\left[\frac{(t'-\mu')}{\sigma'}\right]^2} \qquad \text{(A1.9)}$$

onde:

μ' = Valor médio do logaritmo natural dos tempos até à avaria;

σ' = Desvio padrão do logaritmo natural dos tempos até à avaria.

A função densidade de probabilidade referente à Distribuição Lognormal pode ser representada graficamente, conforme Figura A1.3, onde se pode verificar a influência da média (μ') - Figura A1.3(a) e a influência do desvio-padrão (σ') – Figura A1.3(b).

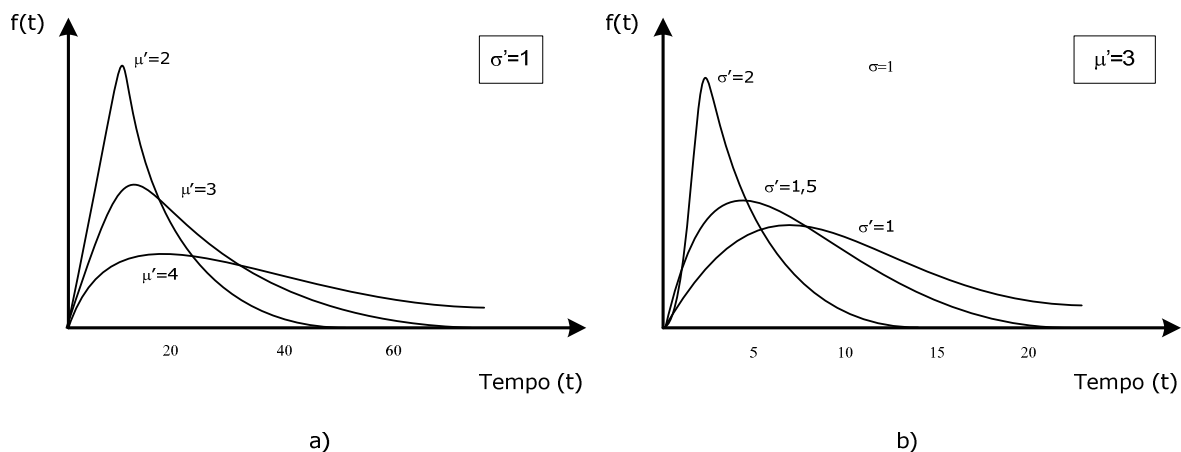



Figura A1.3 – Função densidade de probabilidade para a distribuição Lognormal

A equação da fiabilidade virá dada, por conseguinte, por:

$$R(t) = \int_{t'}^{\infty} \frac{1}{\sigma'.\sqrt{2.\pi}}.e^{-\frac{1}{2}.\left[\frac{(t'-\mu')}{\sigma'}\right]^2}.dt \qquad \text{(A1.10)}$$

À semelhança da distribuição normal, esta expressão também não possui uma solução directa, pelo que poderá ser calculada através de tabelas obtidas por cálculo numérico ou utilizando programas informáticos específicos.

A1.4 – Distribuição Binomial

Também podem ser referidas algumas distribuições discretas, referindo-se a situações onde são apenas possíveis duas saídas, como sobreviver ou falhar, sucesso ou insucesso, como é o caso da distribuição Binomial. A função de densidade de probabilidade discreta para a distribuição Binomial é bi-paramétrica e pode ser representada pela seguinte expressão:

$$f(r) = \binom{n}{r}.p^r.q^{(n-r)} \quad \text{(A1.11)}$$

ou

$$f(r) = \frac{n!}{r!.(n-r)!}.p^r.q^{(n-r)} \quad \text{(A1.12)}$$

onde:

- n = número de ensaios
- r = número de insucessos
- p = probabilidade de insucesso
- q = probabilidade de sucesso

Pode-se calcular a média da distribuição Binomial através da seguinte expressão:

$$\mu = n.p \quad \text{(A1.13)}$$

E o seu desvio padrão por:

$$\sigma = \sqrt{n.p.q} \quad \text{(A1.14)}$$

Por analogia com a expressão A1.13 confirma-se a expressão usada para o cálculo do número médio de avarias $N_f(t)$ referente a uma amostra N_0, representada por:

$$N_f(t) = N_0.F(t) \quad \text{(A1.15)}$$

A função de distribuição Binomial acumulada, ou seja, a probabilidade de se obter "*r*" ou menos insucessos em "*n*" tentativas é dada por:

$$F(r) = \sum_{r=0}^{r} \binom{n}{r} . p^{r} . q^{(n-r)} \qquad \text{(A1.16)}$$

A1.5 - Distribuição de Poisson

A distribuição de Poisson é também uma distribuição discreta. Tal como a distribuição Binomial, refere-se a situações com apenas uma de duas saídas possíveis e onde o acontecimento elementar tem uma probabilidade constante ou taxa de ocorrência constante.

A distribuição de Poisson pode também ser considerada uma extensão da distribuição Binomial, quando a amostra pode ser considerada infinita ($n=\infty$), sendo uma boa aproximação da distribuição Binomial quando "*p*" (probabilidade de insucesso) é relativamente pequena e "*n*" (dimensão da amostra) é relativamente grande (Carinhas, 2007). A função densidade de probabilidade de falha para a distribuição de Poisson é mono-paramétrica (μ) e pode ser determinada a partir da seguinte expressão:

$$f(r) = \frac{\mu^{r}}{r!} . e^{(-\mu)} \qquad \text{(A1.17)}$$

onde:

μ = taxa média de ocorrência do insucesso ($\mu = n.p$)

A função de probabilidade acumulada de falha para a função (discreta) de Poisson é dada por:

$$F(r) = \frac{N_f(t)^{r} . e^{-N_f(t)}}{r!} \qquad \text{(A1.18)}$$

Uma das aplicações da distribuição de Poisson poderá ser na área da gestão de stocks, permitindo na presença da ocorrência aleatória de avarias determinar a probabilidade dos bens em stock darem para satisfazer as respectivas necessidades de substituição num

determinado intervalo de tempo. Assim, procede-se ao cálculo da quantidade de reservas que deverá existir para se obter uma dada probabilidade de cobertura de stock ou nível de qualidade do serviço prestado pelo armazém.

A1.6 - Teste de Laplace

O comportamento das avarias pode ser analisado através do Teste de Laplace, verificando se a taxa de avarias é constante, ou se, pelo contrário, os tempos até à avaria (TTF) apresentam alguma tendência.

Na realidade, os tempos até à avaria registados ao longo do tempo podem estar a aumentar, fruto da melhoria da manutenção ou diminuição da severidade das condições de operação, ou pelo contrário podem estar a diminuir face a processos de degradação, deficiente qualidade da manutenção ou aumento da severidade das condições de exploração, podendo em ambos os casos haver dependência entre as avarias registadas.

O Teste de Laplace serve para verificar o pressuposto de que se trata de um Processo de Poisson Homogéneo (HPP), com tempos até à avaria estatisticamente independentes e identicamente distribuídos. Após a ordenação cronologica dos TTF, este processo passa por seleccionar a estatística de teste (ET) para verificar a veracidade da hipótese nula H_0 (os TTF são independentes entre si ou a taxa de avarias é constante), tendo como hipótese alternativa H_1 (os TTF não são independentes entre si ou a taxa de avarias não é constante). A estatística de teste é uma variável aleatória aproximadamente normal e pode assumir duas formas, conforme seja limitada pelo tempo ou pelo número de avarias, sendo respectivamente calculada através das seguintes expressões (Leitão, 1999):

$$ET = \sqrt{12.N}.\left(\frac{\sum_{i=1}^{N} Ti}{N.T_0} - 0,5 \right) \quad \text{(teste é limitado por tempo)} \qquad \text{(A1.19)}$$

$$ET = \sqrt{12.(N-1)}.\left(\frac{\sum_{i=1}^{N-1} Ti}{(N-1).T_0} - 0,5 \right) \quad \text{(teste é limitado por avaria)} \qquad \text{(A1.20)}$$

Onde:

T_i = Tempo de avaria de ordem "i"

N = Número de avarias / ocorrências acumulado

T_0 = Tempo final (ou total)

Se a taxa de avarias for aproximadamente constante, designa-se por "*Processo de Poisson Homogéneo*" (HPP), caso contrário, é um "*Processo de Poisson Não Homogéneo*" (NHPP). A regra de decisão é especificada em relação a um determinado nível de significância (α). Este valor é definido por nós e corresponde à probabilidade de erradamente se rejeitar a hipótese nula (H_0) quando ela é verdadeira, designando-se este erro por "*Erro Tipo I*", ou à probabilidade de erradamente não rejeitar (aceitar) a hipótese nula (H_0) quando H_1 (hipótese alternativa) é verdadeira, designando-se este erro por "*Erro Tipo II*".

Normalmente α=1%, 5% ou 10%. Este valor de referência (também designado por vezes de valor crítico) é lido na Tabela de Distribuição Normal (ver **Anexo II**) e comparado com o valor da estatística de teste calculado através da expressão A1.19 ou A1.20. Na prática, se estamos a analisar determinados equipamentos e recolhemos os tempos até à avaria nesses equipamentos, utilizamos estes dados e o tempo total de funcionamento do conjunto analisado para obter o valor da ET. Se por exemplo ET=0,2272 e se a regra de decisão for α=5% (bilateral), estamos perante a situação retratada pela Figura A1.4.

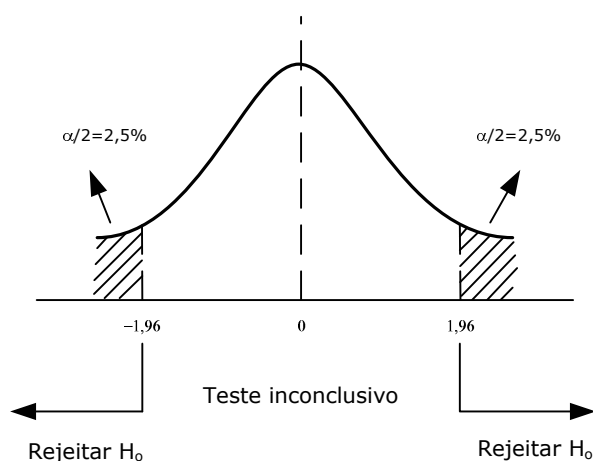



Figura A1.4 – Exemplo gráfico do Teste de Laplace

Como -1,96<ET<1,96 o teste é formalmente inconclusivo. Podemos dizer que não há evidência estatística que permita concluir pela não veracidade da hipótese nula. Neste caso aceita-se H_0 ou tenta-se recolher mais informação (dados).

De qualquer forma podemos recorrer ao Valor de Prova (VP) para verificar a probabilidade de, nas condições da hipótese nula, se obter uma amostra com as características daquela que foi de facto obtida. Se VP>α, aceita-se H_0, caso contrário rejeita-se a hipótese nula. Neste caso verificar-se-ia se:

VP=Prob (ET≥0,2272)

VP=2x0,41

VP=0,82

VP>α

Logo, aceita-se H_0 uma vez que existe 82% de probabilidade de se obter esta amostra no universo de equipamentos (quanto maior o Valor de Prova, mais certeza há de que H_0 é verdade.

Se a hipótese nula for rejeitada e se confirmar que o valor encontrado para ET é inferior ao valor de referência retirado da Tabela Normal correspondente ao nível de significância assumido, a taxa de avarias é decrescente, logo com uma fiabilidade crescente. Nestes casos, o crescimento da fiabilidade pode ser analisado através do modelo de Duane[26] ou modelo de Crow[27]. Caso o valor de ET seja superior estaremos perante um processo de deterioração (taxa de avarias crescente).

---

[26] O modelo de Duane é aplicado principalmente no desenvolvimento de novos produtos, uma vez que nesta fase se pode melhorar progressivamente a sua fiabilidade. Verifica-se que o valor acumulado dos tempos médios entre as falhas em função da duração acumulada do ensaio e da quantidade acumulada de falhas satisfazia uma distribuição tipo exponencial, sendo representada por uma linha praticamente recta com uma inclinação "α"que representa o crescimento da fiabilidade. Trata-se de um modelo determinístico.

[27] O modelo de Crow (ou Crow-AMSAA), desenvolvido pelo Dr. Larry Crow, é o mais frequente e apropriado quando existem várias etapas no desenvolvimento do produto, com as melhorias introduzidas em cada etapa. Admitiu-se que o modelo de Duane podia ser representado estatisticamente através de uma distribuição tipo Weibull biparamétrica. Assim, é um modelo probabilístico elaborado a partir do método AMSAA (*Army Material Systems Analysis Activity*) e do método NHPP (*Non Homogeneous Poisson Process*). Baseia-se na linearidade da variação da intensidade de falhas instantâneas dada por $\lambda(t) = \lambda.\beta.t^{(\beta-1)}$

REFERÊNCIAS (Anexo I)

CARINHAS, H. (2007), *Apontamentos de Fiabilidade*, Instituto Superior de Engenharia de Lisboa

LEITÃO, A., (1999), Notas da Disciplina de Métodos Quantitativos de Gestão, Faculdade de Engenharia da Universidade do Porto

PALLEROSI, C. (2006), *Confiabilidade, a Quarta Dimensão da Qualidade – Conceitos Básicos e Métodos de Cálculo (Volume 1)*, Reliasoft Brasil

ANEXO II

TABELA DA DISTRIBUIÇÃO NORMAL

TABELA DA DISTRIBUIÇÃO NORMAL PADRÃO $\Phi(z) = P(Z<z)$

z	0,0	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
0,0	0,5000	0,5040	0,5080	0,5120	0,5160	0,5199	0,5239	0,5279	0,5319	0,5359
0,1	0,5398	0,5438	0,5478	0,5517	0,5557	0,5596	0,5636	0,5675	0,5714	0,5753
0,2	0,5793	0,5832	0,5871	0,5910	0,5948	0,5987	0,6026	0,6064	0,6103	0,6141
0,3	0,6179	0,6217	0,6255	0,6293	0,6331	0,6368	0,6406	0,6443	0,6480	0,6517
0,4	0,6554	0,6591	0,6628	0,6664	0,6700	0,6736	0,6772	0,6808	0,6844	0,6879
0,5	0,6915	0,6950	0,6985	0,7019	0,7054	0,7088	0,7123	0,7157	0,7190	0,7224
0,6	0,7257	0,7291	0,7324	0,7357	0,7389	0,7422	0,7454	0,7486	0,7517	0,7549
0,7	0,7580	0,7611	0,7642	0,7673	0,7704	0,7734	0,7764	0,7794	0,7823	0,7852
0,8	0,7881	0,7910	0,7939	0,7967	0,7995	0,8023	0,8051	0,8078	0,8106	0,8133
0,9	0,8159	0,8186	0,8212	0,8238	0,8264	0,8289	0,8315	0,8340	0,8365	0,8389
1,0	0,8413	0,8438	0,8461	0,8485	0,8508	0,8531	0,8554	0,8577	0,8599	0,8621
1,1	0,8643	0,8665	0,8686	0,8708	0,8729	0,8749	0,8770	0,8790	0,8810	0,8830
1,2	0,8849	0,8869	0,8888	0,8907	0,8925	0,8944	0,8962	0,8980	0,8997	0,9015
1,3	0,9032	0,9049	0,9066	0,9082	0,9099	0,9115	0,9131	0,9147	0,9162	0,9177
1,4	0,9192	0,9207	0,9222	0,9236	0,9251	0,9265	0,9279	0,9292	0,9306	0,9319
1,5	0,9332	0,9345	0,9357	0,9370	0,9382	0,9394	0,9406	0,9418	0,9429	0,9441
1,6	0,9452	0,9463	0,9474	0,9484	0,9495	0,9505	0,9515	0,9525	0,9535	0,9545
1,7	0,9554	0,9564	0,9573	0,9582	0,9591	0,9599	0,9608	0,9616	0,9625	0,9633
1,8	0,9641	0,9649	0,9656	0,9664	0,9671	0,9678	0,9686	0,9693	0,9699	0,9706
1,9	0,9713	0,9719	0,9726	0,9732	0,9738	0,9744	0,9750	0,9756	0,9761	0,9767
2,0	0,9772	0,9778	0,9783	0,9788	0,9793	0,9798	0,9803	0,9808	0,9812	0,9817
2,1	0,9821	0,9826	0,9830	0,9834	0,9838	0,9842	0,9846	0,9850	0,9854	0,9857
2,2	0,9861	0,9864	0,9868	0,9871	0,9875	0,9878	0,9881	0,9884	0,9887	0,9890
2,3	0,9893	0,9896	0,9898	0,9901	0,9904	0,9906	0,9909	0,9911	0,9913	0,9916
2,4	0,9918	0,9920	0,9922	0,9925	0,9927	0,9929	0,9931	0,9932	0,9934	0,9936
2,5	0,9938	0,9940	0,9941	0,9943	0,9945	0,9946	0,9948	0,9949	0,9951	0,9952
2,6	0,9953	0,9955	0,9956	0,9957	0,9959	0,9960	0,9961	0,9962	0,9963	0,9964
2,7	0,9965	0,9966	0,9967	0,9968	0,9969	0,9970	0,9971	0,9972	0,9973	0,9974
2,8	0,9974	0,9975	0,9976	0,9977	0,9977	0,9978	0,9979	0,9979	0,9980	0,9981
2,9	0,9981	0,9982	0,9982	0,9983	0,9984	0,9984	0,9985	0,9985	0,9986	0,9986
3,0	0,9987	0,9987	0,9987	0,9988	0,9988	0,9989	0,9989	0,9989	0,9990	0,9990
3,1	0,9990	0,9991	0,9991	0,9991	0,9992	0,9992	0,9992	0,9992	0,9993	0,9993
3,2	0,9993	0,9993	0,9994	0,9994	0,9994	0,9994	0,9994	0,9995	0,9995	0,9995
3,3	0,9995	0,9995	0,9995	0,9996	0,9996	0,9996	0,9996	0,9996	0,9996	0,9997
3,4	0,9997	0,9997	0,9997	0,9997	0,9997	0,9997	0,9997	0,9997	0,9997	0,9998
3,5	0,9998	0,9998	0,9998	0,9998	0,9998	0,9998	0,9998	0,9998	0,9998	0,9998
3,6	0,9998	0,9998	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999
3,7	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999
3,8	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999
3,9	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

2 / 2

z	0,0	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
0,0	0,5000	0,4960	0,4920	0,4880	0,4840	0,4801	0,4761	0,4721	0,4681	0,4641
-0,1	0,4602	0,4562	0,4522	0,4483	0,4443	0,4404	0,4364	0,4325	0,4286	0,4247
-0,2	0,4207	0,4168	0,4129	0,4090	0,4052	0,4013	0,3974	0,3936	0,3897	0,3859
-0,3	0,3821	0,3783	0,3745	0,3707	0,3669	0,3632	0,3594	0,3557	0,3520	0,3483
-0,4	0,3446	0,3409	0,3372	0,3336	0,3300	0,3264	0,3228	0,3192	0,3156	0,3121
-0,5	0,3085	0,3050	0,3015	0,2981	0,2946	0,2912	0,2877	0,2843	0,2810	0,2776
-0,6	0,2743	0,2709	0,2676	0,2643	0,2611	0,2578	0,2546	0,2514	0,2483	0,2451
-0,7	0,2420	0,2389	0,2358	0,2327	0,2296	0,2266	0,2236	0,2206	0,2177	0,2148
-0,8	0,2119	0,2090	0,2061	0,2033	0,2005	0,1977	0,1949	0,1922	0,1894	0,1867
-0,9	0,1841	0,1814	0,1788	0,1762	0,1736	0,1711	0,1685	0,1660	0,1635	0,1611
-1,0	0,1587	0,1562	0,1539	0,1515	0,1492	0,1469	0,1446	0,1423	0,1401	0,1379
-1,1	0,1357	0,1335	0,1314	0,1292	0,1271	0,1251	0,1230	0,1210	0,1190	0,1170
-1,2	0,1151	0,1131	0,1112	0,1093	0,1075	0,1056	0,1038	0,1020	0,1003	0,0985
-1,3	0,0968	0,0951	0,0934	0,0918	0,0901	0,0885	0,0869	0,0853	0,0838	0,0823
-1,4	0,0808	0,0793	0,0778	0,0764	0,0749	0,0735	0,0721	0,0708	0,0694	0,0681
-1,5	0,0668	0,0655	0,0643	0,0630	0,0618	0,0606	0,0594	0,0582	0,0571	0,0559
-1,6	0,0548	0,0537	0,0526	0,0516	0,0505	0,0495	0,0485	0,0475	0,0465	0,0455
-1,7	0,0446	0,0436	0,0427	0,0418	0,0409	0,0401	0,0392	0,0384	0,0375	0,0367
-1,8	0,0359	0,0351	0,0344	0,0336	0,0329	0,0322	0,0314	0,0307	0,0301	0,0294
-1,9	0,0287	0,0281	0,0274	0,0268	0,0262	0,0256	0,0250	0,0244	0,0239	0,0233
-2,0	0,0228	0,0222	0,0217	0,0212	0,0207	0,0202	0,0197	0,0192	0,0188	0,0183
-2,1	0,0179	0,0174	0,0170	0,0166	0,0162	0,0158	0,0154	0,0150	0,0146	0,0143
-2,2	0,0139	0,0136	0,0132	0,0129	0,0125	0,0122	0,0119	0,0116	0,0113	0,0110
-2,3	0,0107	0,0104	0,0102	0,0099	0,0096	0,0094	0,0091	0,0089	0,0087	0,0084
-2,4	0,0082	0,0080	0,0078	0,0075	0,0073	0,0071	0,0069	0,0068	0,0066	0,0064
-2,5	0,0062	0,0060	0,0059	0,0057	0,0055	0,0054	0,0052	0,0051	0,0049	0,0048
-2,6	0,0047	0,0045	0,0044	0,0043	0,0041	0,0040	0,0039	0,0038	0,0037	0,0036
-2,7	0,0035	0,0034	0,0033	0,0032	0,0031	0,0030	0,0029	0,0028	0,0027	0,0026
-2,8	0,0026	0,0025	0,0024	0,0023	0,0023	0,0022	0,0021	0,0021	0,0020	0,0019
-2,9	0,0019	0,0018	0,0018	0,0017	0,0016	0,0016	0,0015	0,0015	0,0014	0,0014
-3,0	0,0013	0,0013	0,0013	0,0012	0,0012	0,0011	0,0011	0,0011	0,0010	0,0010
-3,1	0,0010	0,0009	0,0009	0,0009	0,0008	0,0008	0,0008	0,0008	0,0007	0,0007
-3,2	0,0007	0,0007	0,0006	0,0006	0,0006	0,0006	0,0006	0,0005	0,0005	0,0005
-3,3	0,0005	0,0005	0,0005	0,0004	0,0004	0,0004	0,0004	0,0004	0,0004	0,0003
-3,4	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0002
-3,5	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002
-3,6	0,0002	0,0002	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,7	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,8	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,9	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000

ANEXO III

TEORIA DAS PROBABILIDADES

A3 – Teoria das Probabilidades

A3.1 – Introdução

A teoria da probabilidade é a técnica matemática básica utilizada nas análises quantitativas de Árvore de Falhas. É básica uma vez que possibilita um tratamento analítico dos acontecimentos que são a essência de cada Árvore. São de salientar alguns tópicos como os resultados de testes aleatórios, frequências relativas, a álgebra das probabilidades, cálculo combinatório e alguma teoria de conjuntos.

Desta forma, são descritos no presente Anexo algumas matérias relacionadas com a teoria da probabilidade e a álgebra booleana, tendo por base a publicação "*Fault Tree Handbook*" da "*U.S. Nuclear Regulatory Commission*" (1981) (NUREG-0492).

A3.2 – Testes aleatórios e seus resultados

Define-se teste aleatório como qualquer observação, ou conjunto de observações, onde os resultados possíveis são não-determinísticos (se determinístico, então o resultado de uma observação seria sempre o mesmo). Desta forma o resultado será sempre um de vários resultados possíveis (ex. lançamento de um dado ou uma moeda).

O conjunto de todos os resultados possíveis é matematicamente conhecido como o espaço de resultados $\{E_1, E_2, ..., E_n\}$. Por exemplo, se tomarmos como teste o arranque de um motor diesel e o objectivo for determinar se o mesmo falha (F) ou tem sucesso (S), o espaço de resultados será {S, F}.

A3.3 – A frequência relativa

Ao repetir um teste N vezes observa-se a ocorrência do acontecimento E_1 em N_1 casos. Pode-se dizer que a frequência relativa de ocorrência do acontecimento E_1 é dada por:

$$\frac{N_1}{N} \tag{A3.1}$$

Quando N se torna um valor elevado ($N \rightarrow \infty$), designa-se a este limite a probabilidade associada ao acontecimento E_1, ou $P(E_1)$. Assim:

$$P(E_1) = \lim_{N \rightarrow \infty} \left(\frac{N_1}{N} \right) \tag{A3.2}$$

Esta probabilidade possui algumas propriedades, como:

$0<P(E_1)<1$

Se $P(E_1)=1$, então o acontecimento E_1 é certo

Se $P(E_1)=0$, então o acontecimento E_1 é impossível

A3.4 – Operações com probabilidades

Na realização de um teste ou ensaio consideremos a possibilidade de apenas dois resultados, nomeadamente o acontecimento A e o acontecimento B. Suponhamos também que A e B são mutuamente exclusivos (A e B não podem ocorrer em simultâneo). Desta forma, a expressão que traduz a ocorrência de A ou B é dada por:

$$P(A \text{ ou } B) = P(A) + P(B) \tag{A3.3}$$

Esta relação é denominada como a "regra da adição das probabilidades", podendo ser aplicada a acontecimentos mutuamente exclusivos. Para acontecimentos que não são mutuamente exclusivos deverá ser usada uma expressão mais geral para a determinação da probabilidade P(A ou B), tal como mostra a expressão (A3.4).

$$\mathrm{P(A\ ou\ B) = P(A) + P(B) - P(A\ e\ B)} \qquad \text{(A3.4)}$$

Se A e B são mutuamente exclusivos, P(A e B)=0. Note-se que a expressão (A3.3) dá-nos sempre um limite superior da verdadeira probabilidade quando os acontecimentos não são mutuamente exclusivos. A expressão (A3.4) pode ser estendida a um número "n" de acontecimentos, como indicado na expressão (A3.5).

$$\begin{aligned}\mathrm{P(E_1\ ou\ E_2\ ou \ldots ou\ E_n)} &= \sum_{i=1}^{n}\mathrm{P(E_i)} - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\mathrm{P(E_i\ e\ E_j)} + \\ &+ \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1}\sum_{k=j+1}^{n}\mathrm{P(E_i\ e\ E_j\ e\ E_k)} \ldots + (-1)^n.\mathrm{P(E_1\ e\ E_2\ e \ldots e\ E_n)}\end{aligned} \qquad \text{(A3.5)}$$

Se ignorarmos a possibilidade dois ou mais acontecimentos E_i ocorrerem em simultâneo, a expressão anterior reduz-se à denominada equação da "aproximação aos eventos raros", que possui um grau de erro abaixo de 10% relativamente à designada verdadeira probabilidade (conservativo), como apresentado em (A3.6):

$$\mathrm{P(E_1\ ou\ E_2\ ou \ldots ou\ E_n)} = \sum_{i=1}^{n}\mathrm{P(E_i)} \qquad \text{(A3.6)}$$

Se forem considerados dois acontecimentos (A e B) mutuamente independentes, ou seja, a ocorrência (ou não ocorrência) de um acontecimento não tem influência na ocorrência (ou não ocorrência) do outro acontecimento e vice-versa. Desta forma, pode-se escrever a denominada "regra da multiplicação de probabilidades".

$$\mathrm{P(A\ e\ B) = P(A).P(B)} \qquad \text{(A3.7)}$$

Quando estendida a mais acontecimentos, resulta na expressão (A3.8).

$$\mathrm{P(E_1\ e\ E_2\ e \ldots e\ E_n)} = \prod_{i=1}^{n}\mathrm{P(E_i)} \qquad \text{(A3.8)}$$

Quando frequentemente aparecem acontecimentos que não são mutuamente independentes (são mutuamente interdependentes) é normal introduzir-se a noção de probabilidade condicional representada por P(B|A) (probabilidade de B dada a ocorrência de A). Assim, virá:

$$P(A \text{ e } B) = P(A).P(B \mid A) = P(B).P(A \mid B) \qquad \text{(A3.9)}$$

Para "n" acontecimentos teremos:

$$P(E_1 \text{ e } E_2 \text{ e} \ldots \text{e } E_n) = P(E_1).P(E_2 \mid E_1).P(E_3 \mid E_1 \text{ e } E_2). \ldots P(E_n \mid E_1 \text{ e } E_2 \text{ e} \ldots \text{e } E_{n-1}) \qquad \text{(A3.10)}$$

Outro aspecto a ser estudado tem a ver com o cálculo da probabilidade de ocorrência de pelo menos um acontecimento entre um conjunto de acontecimentos mutuamente independentes. Para esta análise deve-se ter em atenção que:

$$P(E_1) + P(\overline{E_1}) = 1 \qquad \text{(A3.11)}$$

Desta forma, pode-se dizer que:

$$P(E_1 \text{ ou } E_2 \text{ ou} \ldots \text{ou } E_n) = 1 - \{[1 - P(E_1)].[1 - P(E_2)]\ldots.[1 - P(E_n)]\} \qquad \text{(A3.12)}$$

Na eventualidade de $P(E_1)=P(E_2)=...=P(E_n)=p$, a expressão anterior pode ser reduzida a:

$$P(E_1 \text{ ou } E_2 \text{ ou} \ldots \text{ou } E_n) = 1 - (1 - p)^n \qquad \text{(A3.13)}$$

A3.5 – Análise combinatória

A análise combinatória permite avaliar as probabilidades de várias combinações de acontecimentos, como por exemplo as avarias de sistemas redundantes. Nesta temática existem dois conceitos que necessitam de uma clarificação prévia sobre as suas diferenças. Trata-se dos conceitos "combinação" e "permutação".

Se for considerado um universo de quatro entidades {A,B,C,D} e aleatoriamente considerarmos três dessas entidades (A, B e D), estes elementos podem ser rearranjados ou permutados em seis formas diferentes: ABC, ADB, BAD, BDA, DAB e DBA. Quando se fala em permutações temos que nos preocupar com a ordem, enquanto quando se fala em combinações esse aspecto não é considerado. Tudo depende da natureza do problema especifico em estudo.

Por exemplo quando se trata da falha de um sistema redundante, pode interessar saber o número de avarias admissível, sem que seja importante a ordem com que as mesmas ocorrem (combinações). Noutros casos, porém, a ordem com que as avarias ocorrem pode ter influência no resultado (permutações).

Considere-se o problema de escolher aleatoriamente uma amostra de dimensão "r" de uma população de dimensão "n". Este processo pode ser efectuado de duas formas: com substituição e sem substituição. Na primeira situação, temos "n" hipóteses para a primeira escolha, "n" para a segunda e assim sucessivamente até se completar o número "r". Desta forma existem "n^r" amostras possíveis de dimensão "r", podendo seleccionar-se itens em duplicado. Na segunda situação (sem substituição) temos "n" hipóteses para a primeira escolha, "n-1" para a segunda até "n-r+1" para a escolha de ordem r. Assim, o número total de amostras diferentes de dimensão "r" será:

$$(n).(n-1).(n-2)...(n-r+1) = (n)_r \quad \text{(A3.14)}$$

Este valor também pode ser definido através de números factoriais, como apresentado na expressão (A3.15).

$$(n)_r = \frac{n!}{(n-r)!} \quad \text{(A3.15)}$$

Esta expressão dá-nos um número de permutações de "r" em "n". Se pretendermos combinações não se deve contar o número de vezes "r!" no qual o número "r" pode ser rearranjado. Assim, o número de combinações de "r" em "n" é dado por:

$$\frac{n!}{(n-r)!.r!} = \binom{n}{r} \quad \text{(A3.16)}$$

Para o exemplo anterior (população A, B, C, D) temos quatro combinações possíveis: "ABC", "ABD", "ACD" e "BCD", resultantes do seguinte cálculo:

$$\frac{n4!}{(n-r)!.r!} = \frac{4!}{1!.3!} = 4$$

E cada uma destas combinações pode ter seis permutações, resultado de:

$$\frac{n!}{(n-r)!} = \frac{4!}{1!} = 24$$

Vejamos um exemplo na área da análise da fiabilidade. Considere-se um sistema com "n" componentes idênticos onde a avaria do mesmo ocorre se avariarem "m" dos "n" componentes. Um sistema terá assim um número de combinações de "m" em "n". Se a probabilidade de falha de qualquer componente for "p", a probabilidade de uma qualquer combinação conduzir à falha do sistema será:

$$p^m.(1-p)^{n-m} \qquad \text{(A3.17)}$$

A probabilidade da falha do sistema devido à avaria de "m" componentes é dada pela expressão (A2.18).

$$\binom{n}{m}.p^m.(1-p)^{n-m} \qquad \text{(A3.18)}$$

Considerando que o sistema também falha se avariarem "m+1", "m+2", ... até "n" componentes, o número de situações de falha do sistema para a avaria de "k" componentes (k=m+1, m+2, ..., n) corresponde ao número de combinações de "k" em "n". Para obter a probabilidade de falha total do sistema adicionamos as probabilidades de falha de "m", "m+1", ... componentes, resultando na expressão da distribuição binomial.

$$\sum_{k=m}^{n}\binom{n}{k}.p^k.(1-p)^{n-k} \qquad \text{(A3.19)}$$

A3.6 – Teoria dos conjuntos

A teoria dos conjuntos é uma abordagem mais geral que permite organizar os acontecimentos resultantes de um ensaio para determinar as probabilidades apropriadas. Consideremos, por exemplo, o lançamento de um dado e os seguintes acontecimentos particulares:

A = número 2

B = número par

C = valor menor que 4

D = qualquer número

E = um número divisível por 7

Cada um destes acontecimentos pode ser considerado como um conjunto retirado do universo {1,2,3,4,5,6}. Assim teremos:

A = {2}

B = {2,4,6}

C = {1,2,3}

D = {1,2,3,4,5,6} (Ω = conjunto universal)

E = ϕ (conjunto vazio)

Desta forma verificamos que o elemento "1" pertence apenas aos conjuntos C e D. Também se verifica que os conjuntos A, B e C são subconjuntos de D e que A é um subconjunto de B e de C. Os diagramas de Venn são um meio gráfico que permite visualizar de uma forma simples a teoria de conjuntos. O conjunto universal é normalmente apresentado por uma forma geométrica rectangular e quaisquer subconjuntos (acontecimentos) são colocados no seu interior. A Figura A3.1 representa o diagrama de Venn do exemplo anterior (lançamento de um dado).

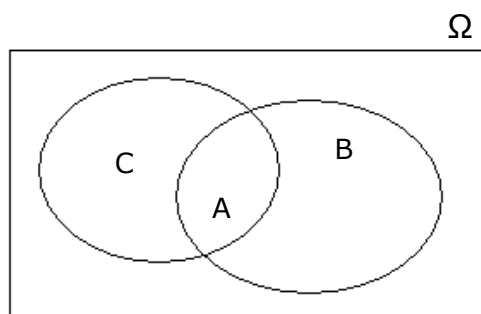



Figura A3.1 – Representação de conjuntos no diagrama de Venn

Nestes diagramas também é possível representar algumas operações como a união de conjuntos, a intersecção de conjuntos ou a complementaridade de conjuntos. A Figura A3.2 mostra a operação referente à união de conjuntos.

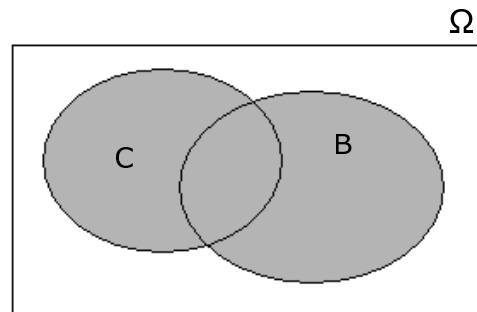



Figura A3.2 – Representação da união de conjuntos

Neste caso ficaria: $B \cup C = \{1,2,3,4,6\}$

A Figura A3.3 mostra a operação referente à intersecção de conjuntos.

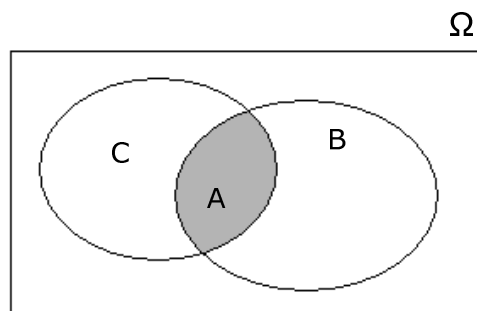



Figura A3.3 – Representação da intersecção de conjuntos

Neste caso ficaria: $B \cap C = \{2\} = A$

A operação de complementaridade encontra-se graficamente representada através da Figura A3.4.

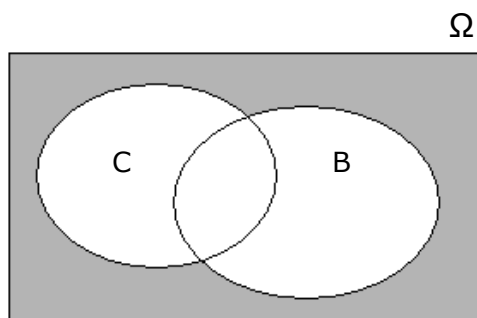



Figura A3.4 – Representação da complementaridade de conjuntos

Para o exemplo referido, o conjunto complementar de $B \cup C = (B \cup C)' = \overline{(B \cup C)} = \{5\}$

Para demonstrar de uma forma simples a teoria de conjuntos toma-se como exemplo um sistema composto por três componentes (X,Y,Z). Como existem três componentes, cada um com dois modos de operação (sucesso e falha), teremos $2^3=8$ combinações que representam todos os modos de falha ou sucesso do sistema. O conjunto universal é dado por:

$$\Omega = \{ABC, \bar{A}BC, A\bar{B}C, AB\bar{C}, \overline{AB}C, A\overline{BC}, \bar{A}B\bar{C}, \overline{ABC}\}$$

Se assumirmos que o sistema falha quando avariam dois ou mais componentes, os acontecimentos correspondentes à falha do sistema são:

$$S_1 = A\overline{BC}$$
$$S_2 = \bar{A}B\bar{C}$$
$$S_3 = \overline{AB}C$$
$$S_4 = \overline{ABC}$$

Então podemos dizer que a falha do sistema é dada pelo subconjunto:

$$S = S_1 \cup S_2 \cup S_3 \cup S_4 = \{A\overline{BC}, \bar{A}B\bar{C}, \overline{AB}C, \overline{ABC}\}$$

A Tabela A3.1 mostra como a álgebra de acontecimentos é representada, de acordo com o campo de aplicação.

Tabela A3.1 – *Simbologia*

Operação	Probabilidade	Matemática	Lógica	Engenharia
União de A com B	A ou B	$A \cup B$	$A \vee B$	A+B
Intersecção de A com B	A e B	$A \cap B$	$A \wedge B$	A.B ou AB
Complementar de A	Não A	A' ou $\bar{A}$	-A	A' ou $\bar{A}$

A álgebra Booleana, aplicada principalmente em Árvores de Falhas, é extremamente importante em situações que envolvam uma dicotomia, como por exemplo, válvula aberta ou fechada, interruptores abertos ou fechados e ocorrência de acontecimento ou

não ocorrência. Um Árvore de Falhas não é mais que uma representação gráfica das relações Booleanas entre acontecimentos tipo avaria que podem provocar a ocorrência do acontecimento de topo. A Tabela A3.2 mostra as regras da álgebra de Boole, podendo-se recorrer aos diagramas de Venn para validar cada uma das regras apresentadas.

Tabela A3.2 – *Regras da álgebra de Boole*

Simbologia matemática	Simbologia de Engenharia	Designação
$X \cap Y = Y \cap X$	$X.Y=Y.X$	Comutativa
$X \cup Y = Y \cup X$	$X+Y=Y+X$	Comutativa
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X.(Y.Z)=(X.Y).Z$	Associativa
$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X+(Y+Z)=(X+Y)+Z$	Associativa
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X.(Y+Z)=X.Y+X.Z$	Distributiva
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X+Y.Z=(X+Y).(X+Z)$	Distributiva
$X \cap X = X$	$X.X=X$	Idempotência
$X \cup X = X$	$X+X=X$	Idempotência
$X \cap (X \cup Y) = X$	$X.(X+Y)=X$	Absorção
$X \cup (X \cap Y) = X$	$X+X.Y=X$	Absorção
$X \cap X' = \phi$	$X.X'=0$	Complementaridade
$X \cup X' = \Omega$	$X+X'=\Omega$	Complementaridade
$(X')'=X$	$(X')'=X$	Complementaridade
$(X \cap Y)' = X' \cup Y'$	$(X.Y)'=X'+Y'$	Teorema de de Morgan
$(X \cup Y)' = X' \cap Y'$	$(X+Y)'=X'.Y'$	Teorema de de Morgan
$\phi \cap X = \phi$	$\phi.X=\phi$	Operações com ϕ e Ω
$\phi \cup X = X$	$\phi+X=X$	Operações com ϕ e Ω
$\Omega \cap X = X$	$\Omega.X=X$	Operações com ϕ e Ω
$\Omega \cup X = \Omega$	$\Omega+X=\Omega$	Operações com ϕ e Ω
$\phi' = \Omega$	$\phi'=\Omega$	Operações com ϕ e Ω
$\Omega' = \phi$	$\Omega'=\phi$	Operações com ϕ e Ω
$X \cup (X' \cap Y) = X \cup Y$	$X+X'.Y=X+Y$	
$X' \cap (X \cup Y') = X' \cap Y' = (X \cup Y)'$	$X'.(X+Y')=X'.Y'=(X+Y)'$	

REFERÊNCIAS (Anexo III)

U.S. NUCLEAR REGULATORY COMMISSION (1981), *Fault Tree Handbook*, NUREG-0492, Washington

FIABILIDADE DE SISTEMAS

A4 – Fiabilidade de Sistemas

A4.1 - Sistemas Série

Num sistema série, os componentes estão relacionados de tal forma que a avaria de um qualquer componente provoca a falha do sistema. Dito de outra forma, pode-se referir que o sucesso do sistema depende do sucesso de todos os seus componentes. Um sistema série pode ser representado graficamente conforme ilustrado na Figura A4.1.

Figura A4.1 – Sistema com arranjo lógico tipo Série

Para um sistema exclusivamente com componentes num arranjo lógico tipo série, a sua fiabilidade é dada por:

$$R_S(t) = \prod_{i=1}^{n} R_i(t) = R_1(t).R_2(t)...R_n(t) \qquad \text{(A4.1)}$$

E a complementar probabilidade acumulada de falha:

$$F_S(t) = 1 - R_S(t) = 1 - \prod_{i=1}^{n} R_i(t) \qquad \text{(A4.2)}$$

Assumindo saber-se a distribuição referente a cada componente, e a expressão relativa à fiabilidade para cada distribuição descrita em parágrafos anteriores, é possível determinar a fiabilidade do sistema através da expressão A4.1.

A4.2 - Sistemas Paralelo

Num sistema paralelo, só ocorre a falha do sistema quando todos os seus componentes avariarem. Também dito de outra forma, pode-se afirmar que um sistema com componentes exclusivamente em paralelo terá sucesso enquanto pelo menos um dos seus componentes o tiver. Um sistema paralelo poderá ser representado conforme Figura A4.2.

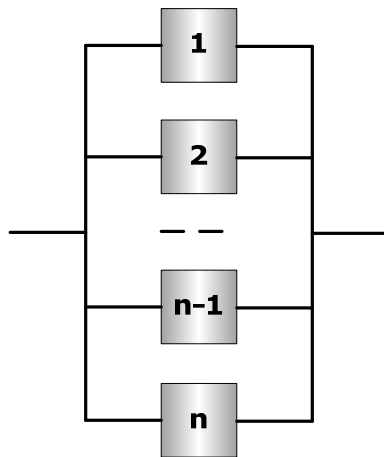



Figura A4.2 – Sistema com arranjo lógico tipo Paralelo Activo

Para um sistema paralelo activo, a fiabilidade do sistema é dada por:

$$R_S(t) = 1 - \prod_{i=1}^{n} F_i(t) = 1 - \left[F_1(t).F_2(t)...F_n(t)\right] \qquad \text{(A4.3)}$$

Sendo a sua probabilidade acumulada de falha calculada através da seguinte expressão:

$$F_S(t) = \prod_{i=1}^{n} F_i(t) = \left[F_1(t).F_2(t)...F_n(t)\right] \qquad \text{(A4.4)}$$

Neste tipo de sistema, designado como paralelo activo, pressupõe-se que todos os componentes que se encontram no arranjo lógico se encontram a funcionar, embora apenas um deles seja necessário para o cumprimento da função do sistema.

No entanto, existe um tipo particular de sistemas paralelos que se refere a situações em que dos "*n*" componentes que se encontram em paralelo necessitamos que pelo menos "*k*" componentes ($k<n$) funcionem para que o sistema funcione. A Figura A4.3 traduz a representação gráfica deste tipo de sistemas, designados por sistemas paralelo restrito ou sistemas paralelo *k* em *n*.

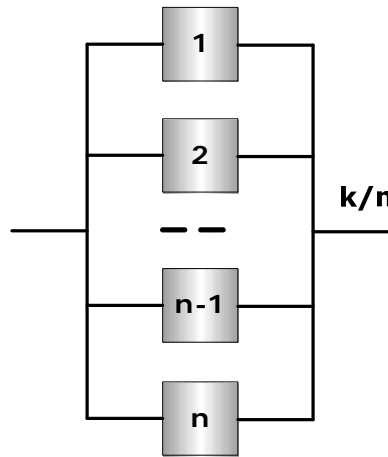



Figura A4.3 – Sistema com arranjo lógico tipo Paralelo Restrito (k/n)

Para arranjos tipo paralelo restrito (k/n), com componentes estatisticamente independentes, a fiabilidade do sistema pode ser determinada através do binómio de Newton ou pela seguinte expressão:

$$R_S(t) = 1 - \sum_{i=1}^{k} \frac{n!}{(i-1)!.(n-i+1)!} . R_i(t)^{i-1} . \left[\prod_{i=1}^{n-i+1} (1 - R_i(t))\right] \qquad \text{(A4.5)}$$

No caso dos componentes serem todos iguais (situação comum no uso de redundâncias), esta expressão simplifica-se, sendo mais prático o cálculo da fiabilidade do sistema paralelo restrito através do Binómio de Newton, incluindo apenas os elementos que

satisfaçam a restrição imposta (k/n) relativamente a todos os estados possíveis. A equação 2.38 refere-se a todas as possibilidades de estados para um exemplo de três componentes idênticos instalados em paralelo.

$$(R+F)^3 = R_1.R_2.R_3 + (R_1.R_2.F_3 + R_1.F_2.R_3 + F_1.R_2.R_3) + (R_1.F_2.F_3 + F_1.R_2.F_3 + F_1.F_2.R_3) + F_1.F_2.F_3 = 1 \quad \text{(A4.6)}$$

ou

$$(R+F)^3 = R^3 + 3R^2F + 3RF^2 + F^3 = 1 \quad \text{(A4.7)}$$

Assim, para o exemplo acima referido, a fiabilidade de um sistema paralelo restrito onde seja necessário no mínimo que dois dos três componentes se encontrem operacionais (2 em 3) pode ser determinada com recurso à seguinte expressão:

$$Rs(t) = R^3 + 3R^2F = 1 - 3RF^2 + F^3 \quad \text{(A4.8)}$$

A4.3 - Sistemas em paralelo *standby*

Devido a algumas considerações técnicas e económicas, podem ser projectados e construídos sistemas onde as redundâncias não se encontram activas[28]. Estes componentes são designados redundâncias passivas ou elementos de socorro e só entrarão em funcionamento quando o respectivo componente primário avariar e haja a informação de um dispositivo denominado detector-comutador (ou sensor-comutador).

Neste tipo de sistemas, relativamente aos detectores-comutadores, e apesar de os mesmos normalmente possuírem altas fiabilidades, também deverão ser considerados os modos de falha e suas probabilidades. Para estes dispositivos, as duas funções básicas (detecção e comutação) são tratadas como se tratasse de um sistema série entre as mesmas, uma vez que é necessário que o equipamento detecte a falha do componente activo **e** que comute para o componente de socorro que se encontra em *standby*.

[28] Significa componentes em funcionamento permanente, independentemente de ser(em) considerado(s) componente(s) primário(s) ou redundância ao(s) primário(s)

Este tipo de redundância é muito utilizado em sistemas de segurança e protecção, ou sistemas tolerantes à falha (FTS - *fault tolerant systems*). A Figura A4.4 representa um sistema paralelo *standby* com "*n*" componentes.

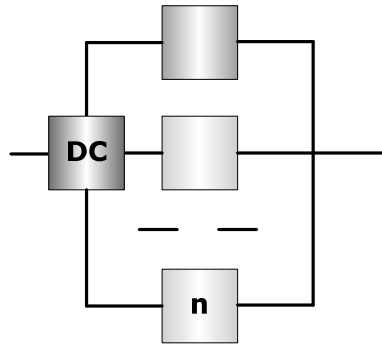



Figura A4.4 – Sistema paralelo tipo standby

O cálculo da fiabilidade de um sistema paralelo tipo *standby*, não é uma tarefa simples. Por exemplo, para um sistema composto unicamente por dois componentes, e tendo em consideração as diversas probabilidades de falha, a fiabilidade pode ser determinada com recurso à seguinte expressão (Carinhas, 2007):

$$R_S(t) = e^{-\lambda_1 . t} + \frac{\lambda_1 . e^{-\lambda_{DCa} . 1} . e^{-\lambda_{2c} . t}}{\lambda_1 + \lambda_{DCd} + \lambda_{2v} - \lambda_{2c}} . \left[1 - e^{-(\lambda_1 + \lambda_{DCd} + \lambda_{2v} - \lambda_{2c}).t}\right] \quad \text{(A4.9)}$$

onde:
λ_1 = Taxa de avarias do componente 1
λ_{2v} = Taxa de avarias do componente 2 em vazio
λ_{2c} = Taxa de avarias do componente 2 em carga
λ_{DCa} = Taxa de avarias do detector-comutador na actuação
λ_{DCd} = Taxa de avarias do detector-comutador quando em detecção

Na eventualidade de existirem "*k*" componentes idênticos num sistema tipo "*standby*", onde o detector-comutador e o componente redundante (quando em vazio) possam possuir taxas de avarias consideradas desprezáveis, a fiabilidade deste sistema pode ser calculada através da expressão A4.10, que não é mais do que a equação referente à distribuição de probabilidade acumulada de Poisson.

$$R_S(t) = e^{-\lambda.t}.\sum_{k=0}^{K}\frac{(\lambda.t)^k}{k!} \qquad \text{(A4.10)}$$

Considerando:

$\lambda_1 = \lambda_2$ e $\lambda_{DCa} \cong \lambda_{DCd} \cong \lambda_{2v} \cong 0$

Nas condições enunciadas anteriormente, e que permitiram utilizar a expressão A4.10 no cálculo da fiabilidade de dois componentes, pode-se generalizar a equação para um sistema *standby* composto por "*n*" componentes idênticos, através da expressão da probabilidade acumulada de Poisson, onde se podem aceitar um máximo de "*n*-1" avarias.

$$R_S(t) = \sum_{k=0}^{n-1}\frac{(\lambda.t)^k.e^{-\lambda.t}}{k!} \qquad \text{(A4.11)}$$

A4.4 - Sistemas mistos

Os sistemas mistos, também designados de compostos ou combinados, correspondem a sistemas constituídos por componentes que se encontram em série e outros componentes associados em paralelo. A Figura A4.5 mostra um exemplo de sistema misto.

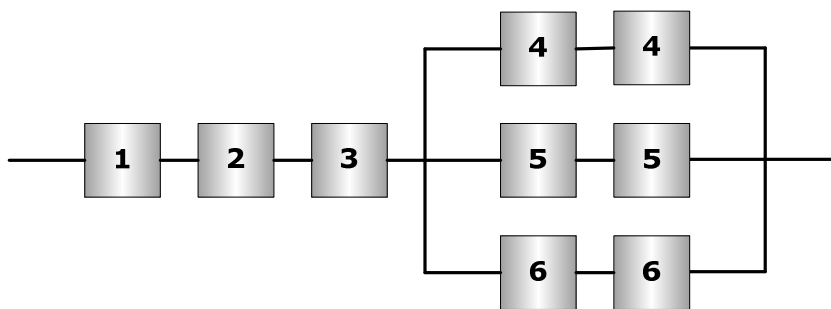



Figura A4.5 – Sistema com arranjo lógico misto

Neste caso, a determinação do valor da fiabilidade do sistema terá por base os subsistemas tipo série e tipo paralelo, calculados individualmente, tal como indicado em A4.1 e A4.2.

Para o exemplo da figura anterior poder-se-ia proceder da seguinte forma:

a) Cálculo da fiabilidade do subsistema série com os componentes "1", "2" e "3";
b) Cálculo da fiabilidade do subsistema série com os componentes "4";
c) Cálculo da fiabilidade do subsistema série com os componentes "5";
d) Cálculo da fiabilidade do subsistema série com os componentes "6";
e) Cálculo da fiabilidade do subsistema paralelo dos subsistemas calculados em b), c) e d);
f) Cálculo da fiabilidade do sistema série composto pelos subsistemas calculados em a) e em e).

Existem situações específicas de sistemas mistos, como as representadas nas Figuras A4.6 e A4.7, respectivamente designados por sistemas série de paralelos e sistemas paralelo de séries.

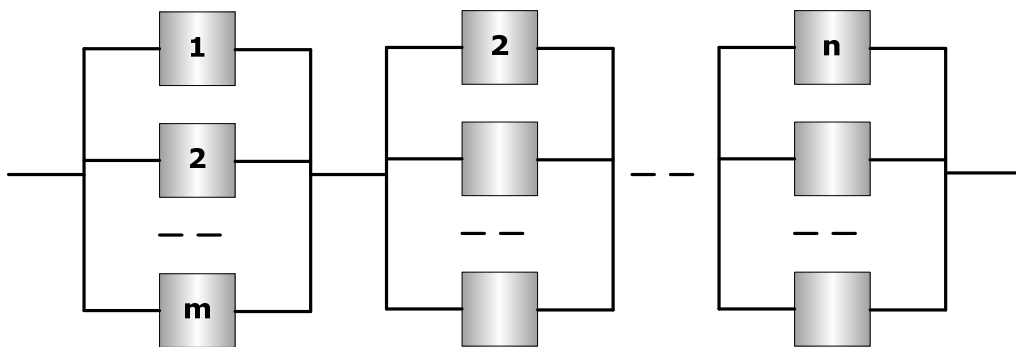



Figura A4.6 – Sistema série de paralelos

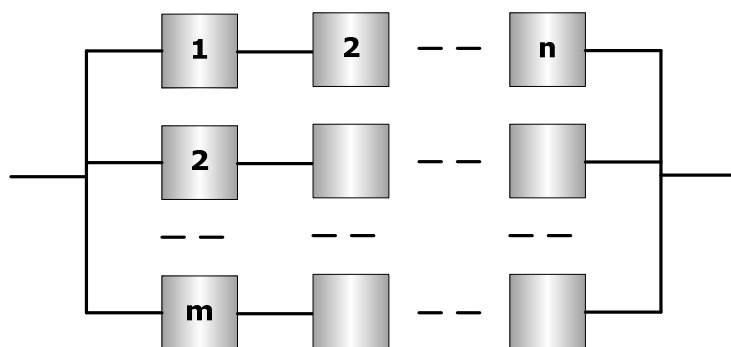



Figura A4.7 – Sistema paralelo de séries

Num sistema série de paralelos, com uma série de "*n*" paralelos, cada um com "*m*" componentes idênticos em paralelo, a fiabilidade do sistema pode ser calculada através da seguinte expressão:

$$R_S(t) = \left[1 - \left[1 - R(t)\right]^m\right]^n \quad \text{(A4.12)}$$

Num sistema paralelo de séries, com um paralelo de "*m*" séries, cada uma com "*n*" componentes idênticos em série, a fiabilidade do sistema pode ser calculada através da seguinte expressão:

$$R_S(t) = 1 - \left[1 - R(t)^n\right]^m \quad \text{(A4.13)}$$

A4.5 - Sistemas complexos ou sistemas cruzados

Considera-se um sistema complexo quando não é possível repartir o sistema em séries, paralelos, série de paralelos ou paralelo de séries, paralelos restritos ou paralelos "*standby*". A Figura A4.8 mostra um exemplo de um sistema complexo, por vezes também denominado sistema cruzado.

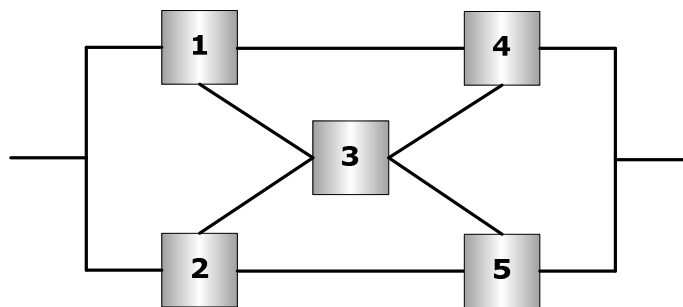



Figura A4.8 – Sistema Complexo

Para o cálculo da fiabilidade deste tipo de sistemas fica apenas a referência a alguns métodos que permitem a sua determinação, tais como:

- Método da Decomposição;
- Método dos Acontecimentos Espaciais;
- Método dos Caminho Críticos.

REFERÊNCIAS (Anexo IV)

CARINHAS, H. (2007), *Apontamentos de Fiabilidade*, Instituto Superior de Engenharia de Lisboa

ANEXO V

ÁRVORE DE FALHAS DA BARREIRA DE SEGURANÇA

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha no Arranque da Central de Bombagem de Água Contra Incêndios
AT
Falha dos Equipamentos de Bombagem
AI1
Válvula de Seccionamento à Saída do Colector de Compressão Fechada - Erro Humano
AB14
Falha no Arranque da Electrobomba Principal
AI2
Falha no Arranque da Motobomba Diesel
AI3
Falha de Energia no Quadro Eléctrico da Electrobomba Principal
AI4
From Page 2
Falha na Transmissão de Potência do Quadro Eléctrico para o Motor Eléctrico
AI5
From Page 3
Falha dos Sensores de Pressão da Electrobomba Principal
AI6
From Page 4
Falha no Motor Eléctrico da Electrobomba Principal
AI7
Impulsor da Electrobomba Principal Preso
AB15
Falha na Transmissão de Potência do Quadro Eléctrico para o Motor Diesel
AI10
Falha dos Sensores de Pressão da Motobomba Diesel
AI11
From Page 5
Falha do Motor Diesel
AI12
From Page 6
Impulsor da Motobomba Diesel Preso
AB21
Falha no Estator/Rotor da Electrobomba Principal
AB12
Rolamentos da Electrobomba Principal Gripados/Agarrados
AB13
Terminais dos Equip. Electromecânicos no Q.E. da Motobomba Diesel Soltos/Partidos
AB16
Falha nos Equip. Electromecânicos do Q.E. da Motobomba Diesel
AB17
Falha no Acoplamento entre o Motor Diesel e a Bomba da Motobomba Diesel
AB18

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha de Energia no Quadro Eléctrico da Electrobomba Principal
AI4
To Page 1
Falha de Energia da Rede Eléctrica Nacional
AB1
Falha de Energia da Rede de Emergência
AI8
Falha do Inversor no QGBT
AB2
Falha do Gerador de Emergência
AI9
Falha Interna do Gerador de Emergência
AB3
Falha no Abastecimento de Combustível ao Gerador de Emergência
AB4

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha na Transmissão de Potência do Quadro Eléctrico para o Motor Eléctrico
AI5
To Page 1
Terminais dos Equip. Electromecânicos no Q.E. da Electrobomba Principal Soltos/Partidos
AB5
Falha nos Equip. Electromecânicos do Q.E. da Electrobomba Principal
AB6
Cablagem entre o Q.E. da Electrobomba Principal e o Motor Eléctrico Interrompida
AB7
Terminais no Motor Eléctrico da Electrobomba Principal Soltos/Partidos
AB8
Falha no Acoplamento entre o Motor Eléctrico e a Bomba da Electrobomba Principal
AB9

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha dos Sensores de Pressão da Electrobomba Principal
AI6
To Page 1
Falha no Pressostato de Arranque da Electrobomba Principal
AB10
Falha no Pressostato de Segurança da Electrobomba Principal
AB11

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha dos Sensores de Pressão da Motobomba Diesel
AI11
To Page 1
Falha no Pressostato de Arranque da Motobomba Diesel
AB19
Falha no Pressostato de Segurança da Motobomba Diesel
AB20

Relex
Fault Tree Diagram
File Name: PhD Thesis Sobral v1.rfp
Falha do Motor Diesel
AI12
To Page 1
Falha do Motor de Arranque da Motobomba Diesel
AI13
Motor Diesel da Motobomba Diesel Gripado/Agarrado
AB22
Falha na Alimentação de Combustível à Motobomba Diesel
AI15
Falha das Baterias de Arranque da Motobomba Diesel
AI14
Falha das Escovas do Motor de Arranque da Motobomba Diesel
AB25
Falta de Combustível no Depósito da Motobomba Diesel
AB26
Combustível Congelado no Depósito ou nas Tubagens de Ida e Retorno
AB27
Combustível Deteriorado no Depósito da Motobomba Diesel
AB28
Tubagens de Ida e Retorno do Depósito de Combustível Interrompidas ou Desligadas
AB29
Falha da Bateria "A" da Motobomba Diesel
AB23
Falha da Bateria "B" da Motobomba Diesel
AB24

ANEXO VI

CONJUNTOS DE CORTE MÍNIMOS (MCS)

Relex

Fault Tree Cut Sets

File Name: PhD Thesis Sobral v1.rfp

Top Gate: AT

Events	Cutset Order	Unavailability	Unreliability
AB14	1		
AB12, AB27	2		
AB12, AB26	2		
AB12, AB25	2		
AB12, AB22	2		
AB12, AB21	2		
AB12, AB18	2		
AB12, AB17	2		
AB9, AB16	2		
AB9, AB29	2		
AB13, AB16	2		
AB9, AB28	2		
AB9, AB27	2		
AB9, AB26	2		
AB9, AB25	2		
AB9, AB22	2		
AB9, AB21	2		
AB9, AB18	2		
AB9, AB17	2		
AB12, AB16	2		
AB13, AB28	2		
AB15, AB29	2		
AB15, AB28	2		
AB15, AB27	2		
AB15, AB26	2		
AB15, AB25	2		
AB15, AB22	2		
AB15, AB21	2		
AB12, AB28	2		
AB13, AB29	2		
AB12, AB29	2		
AB13, AB27	2		
AB13, AB26	2		
AB13, AB25	2		
AB13, AB22	2		
AB13, AB21	2		
AB13, AB18	2		
AB13, AB17	2		
AB15, AB16	2		
AB15, AB17	2		
AB5, AB27	2		
AB6, AB27	2		
AB6, AB26	2		
AB6, AB25	2		
AB6, AB22	2		
AB6, AB21	2		
AB6, AB18	2		
AB6, AB17	2		
AB6, AB16	2		

Relex

Fault Tree Cut Sets

File Name: PhD Thesis Sobral v1.rfp

Top Gate: AT

Events	Cutset Order	Unavailability	Unreliability
AB6, AB28	2		
AB5, AB28	2		
AB5, AB26	2		
AB5, AB25	2		
AB5, AB22	2		
AB5, AB21	2		
AB5, AB18	2		
AB5, AB17	2		
AB5, AB16	2		
AB8, AB29	2		
AB15, AB18	2		
AB5, AB29	2		
AB8, AB21	2		
AB8, AB28	2		
AB8, AB27	2		
AB6, AB29	2		
AB8, AB26	2		
AB8, AB22	2		
AB8, AB18	2		
AB8, AB17	2		
AB8, AB16	2		
AB7, AB29	2		
AB7, AB18	2		
AB7, AB27	2		
AB7, AB16	2		
AB7, AB26	2		
AB7, AB25	2		
AB7, AB17	2		
AB7, AB22	2		
AB7, AB21	2		
AB7, AB28	2		
AB8, AB25	2		
AB10, AB11, AB17	3		
AB10, AB11, AB16	3		
AB9, AB23, AB24	3		
AB9, AB19, AB20	3		
AB8, AB23, AB24	3		
AB8, AB19, AB20	3		
AB7, AB23, AB24	3		
AB6, AB23, AB24	3		
AB6, AB19, AB20	3		
AB10, AB11, AB18	3		
AB12, AB23, AB24	3		
AB5, AB23, AB24	3		
AB5, AB19, AB20	3		
AB7, AB19, AB20	3		
AB10, AB11, AB21	3		
AB10, AB11, AB22	3		
AB10, AB11, AB25	3		

Relex

Fault Tree Cut Sets

File Name: PhD Thesis Sobral v1.rfp

Top Gate: AT

Events	Cutset Order	Unavailability	Unreliability
AB10, AB11, AB26	3		
AB10, AB11, AB27	3		
AB10, AB11, AB28	3		
AB15, AB23, AB24	3		
AB12, AB19, AB20	3		
AB13, AB19, AB20	3		
AB13, AB23, AB24	3		
AB15, AB19, AB20	3		
AB1, AB4, AB29	3		
AB1, AB3, AB16	3		
AB10, AB11, AB29	3		
AB1, AB2, AB29	3		
AB1, AB2, AB16	3		
AB1, AB2, AB17	3		
AB1, AB2, AB18	3		
AB1, AB2, AB21	3		
AB1, AB2, AB22	3		
AB1, AB2, AB25	3		
AB1, AB2, AB26	3		
AB1, AB3, AB18	3		
AB1, AB2, AB28	3		
AB1, AB4, AB28	3		
AB1, AB3, AB17	3		
AB1, AB3, AB21	3		
AB1, AB3, AB22	3		
AB1, AB4, AB25	3		
AB1, AB2, AB27	3		
AB1, AB4, AB26	3		
AB1, AB3, AB25	3		
AB1, AB4, AB22	3		
AB1, AB4, AB21	3		
AB1, AB4, AB18	3		
AB1, AB4, AB17	3		
AB1, AB4, AB16	3		
AB1, AB3, AB29	3		
AB1, AB3, AB28	3		
AB1, AB3, AB27	3		
AB1, AB3, AB26	3		
AB1, AB4, AB27	3		
AB10, AB11, AB23, AB24	4		
AB1, AB2, AB19, AB20	4		
AB1, AB2, AB23, AB24	4		
AB1, AB3, AB19, AB20	4		
AB1, AB3, AB23, AB24	4		
AB1, AB4, AB19, AB20	4		
AB1, AB4, AB23, AB24	4		
AB10, AB11, AB19, AB20	4		